

DEFENSE INFORMATION SYSTEMS AGENCY

JOINT INTEROPERABILITY TEST COMMAND
FORT HUACHUCA, ARIZONA

Session Border Controller (SBC)

Test Procedures Version 1.0

For

Unified Capabilities Requirements (UCR) 2013 Errata 1

October 2014

Session Border Controller (SBC)

Test Procedures Version 1.0

For

Unified Capabilities Requirements (UCR) 2013 Errata 1

OCTOBER 2014

Submitted by:

Joseph T. Schulte
Chief
Network Systems Branch

Approved by:

LOPEZ.GERARDO.B.1231464928

Digitally signed by LOPEZ.GERARDO.B.1231464928
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=DISA, cn=LOPEZ.GERARDO.B.1231464928
Date: 2014.10.15 21:36:48 -07'00'

GERARDO B. LOPEZ
Technical Director
Networks/Communications and UC Portfolio

Prepared Under the Direction of:

Major James M. Torres
Joint Interoperability Test Command
Fort Huachuca, Arizona

Revision History

Version	Date	Approved By	Comments
1.0	15 October 2014	Gerardo B. Lopez	Original. Based on UCR 2013 Errata 1 signed July 2013.

Errata

Version	Changes

(This page left intentionally blank.)

TABLE OF CONTENTS

Page

LIST OF FIGURES

LIST OF TABLES

INTRODUCTION

The Session Border Controller (SBC), formerly known as the Edge Boundary Controller (EBC), acts as a stateful, AS-SIP-aware application firewall that provides Intrusion Detection System/Intrusion Prevention System (IDS/IPS), Network Address Translation (NAT), and port pinholes for individual voice and video sessions. The SBC acts as AS-SIP Back-to-Back User Agent (B2BUA).

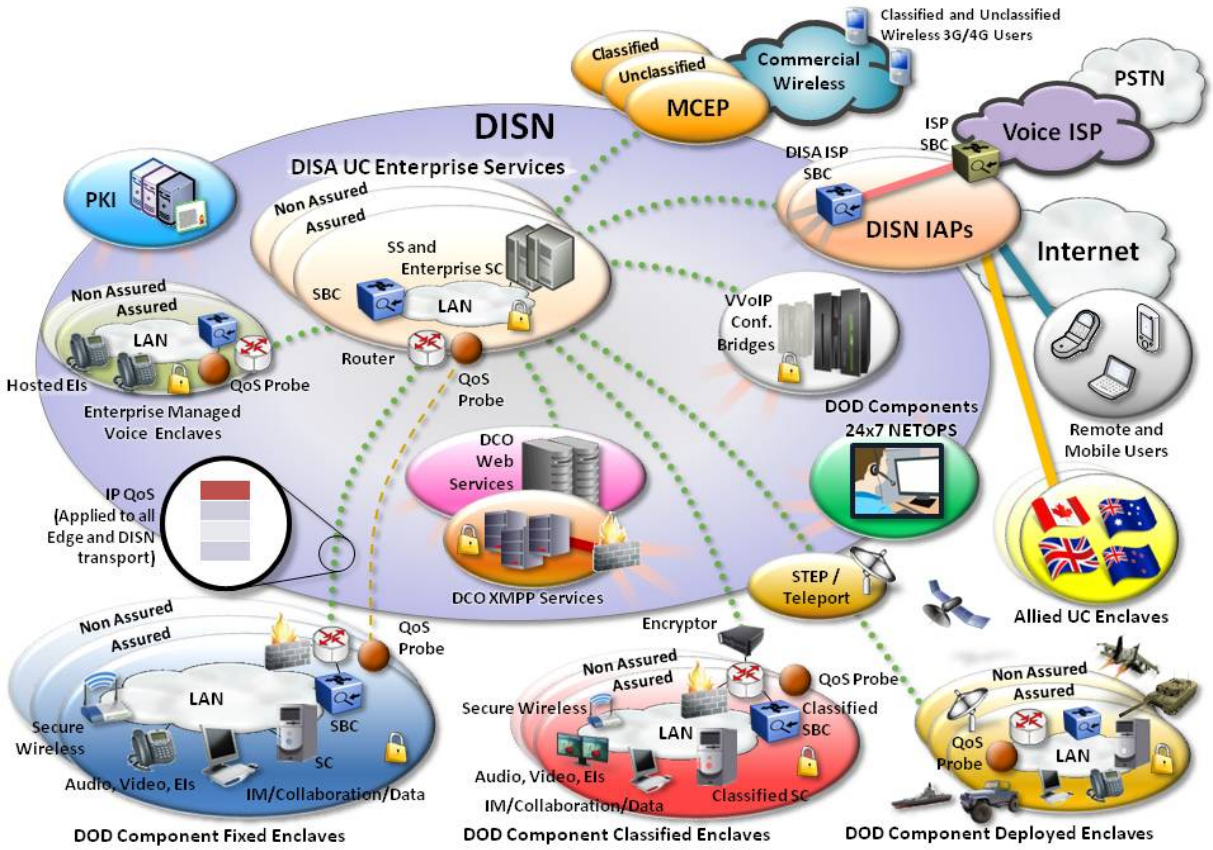
TEST METHODOLOGY

The test methodology used to certify SBCs for UC Approved Products List (APL) placement includes verification of Unified Capabilities Requirements (through a combination of Letters of Compliance (LoC) and functional testing. Demonstration of Information Assurance (IA), interface, and functional capability requirements in a realistic, but non-operational network, results in a characterization of the system under test's ability to meet the SBC requirements found in the UCR. The local test network of the JITC consists of an APL Assured Services Local Area Network (ASLAN) infrastructure, Session Controllers, SBCs, and a variety of end user instruments (voice, video, and collaboration).

The use of Test, Measurement, Diagnostic Equipment (TMDE), such as packet capture and analysis software, ITKO LISA, Spirent, Ixia, Wireshark, and Agilent, are examples of products used to simulate and analyze various data exchanges, and will be used whenever feasible within this test effort to assess functional interoperability (IO). TMDE will be mainly used in the loading and the stimulation of traffic used to assess functional interoperability.

In addition to testing functional capabilities, demonstration or inspection of the system under test to verify requirements shall be carried out. An analysis of the vendor's LoC shall be conducted to verify that requirements marked as "Required" have been met.

Figure 1 illustrates SBC Connectivity in the DoD Operational Framework. Figure 2 illustrates the test architecture for the System under Test (SUT). Figure 3 illustrates the principal of media anchoring at the SBC, while Figure 4 depicts a Wireshark capture of the "c" and "m" lines during media anchoring.



LEGEND:

ASLAN	Assured Services Local Area Network
AS-SIP	Assured Services Session Initiation Protocol
DCO	Defense Connection Online
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DISR	Department of Defense Information Technology Standards Registry
EBC	Edge Boundary Controller
EI	End Instrument
IP	Internet Protocol
IPSec	Internet Protocol Security
ISP	Internet Service Provider
LSC	Local Session Controller
MFSS	Multifunction Softswitch
NETOPS	Network Operations
PKI	Public Key Infrastructure
QoS	Quality of Service
SBC	Session Border Controller
SRTP	Secure Real-Time Transport Protocol
SS	Softswitch
SSL	Secure Socket Layer
TLS	Transport Layer Security
UC	Unified Capabilities
VLAN	Virtual Local Area Network
VVoIP	Voice and Video over IP
XMPP	Extensible Messaging and Presence Protocol

Figure 1. Session Border Controller (SBC) Minimum Capability Architecture

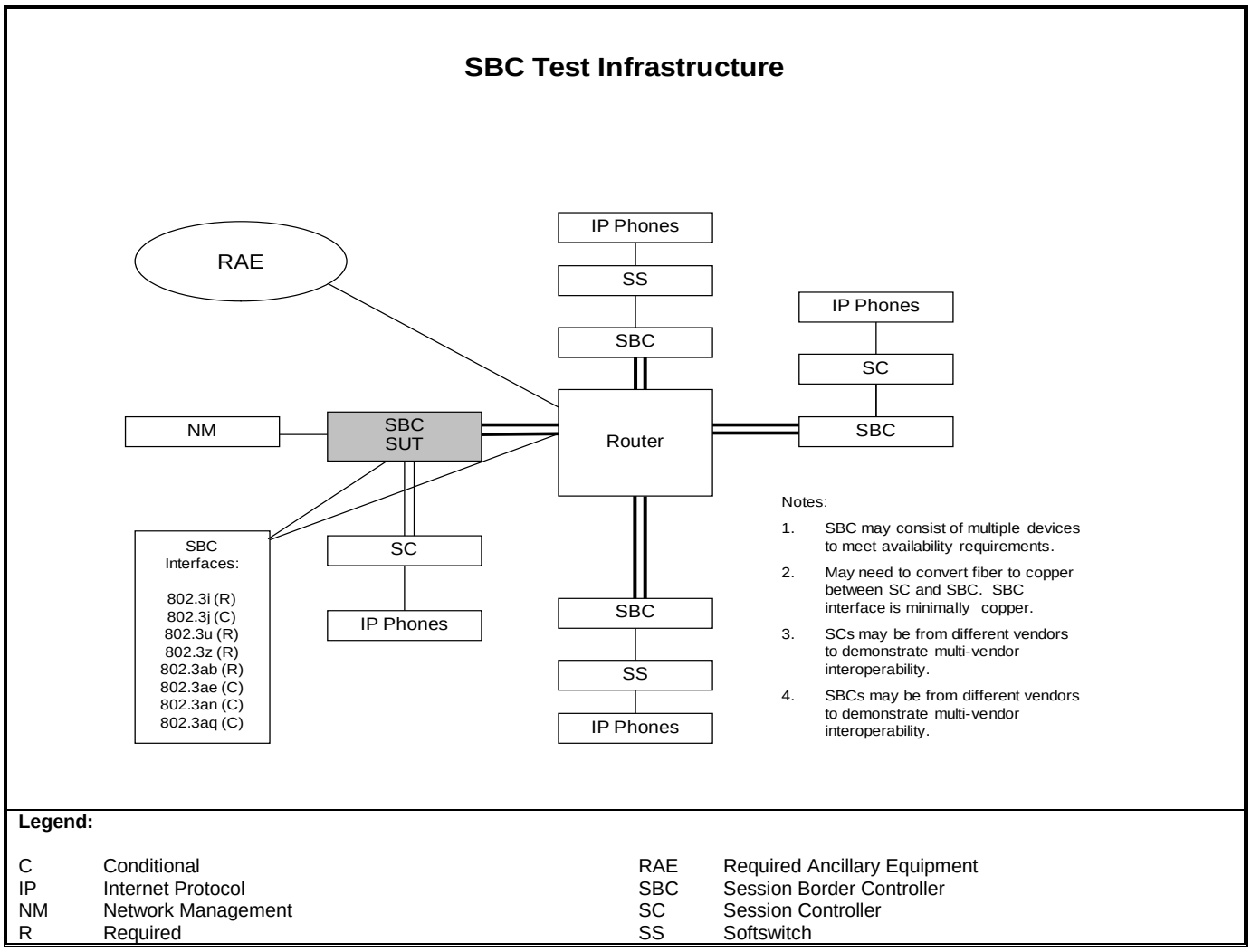
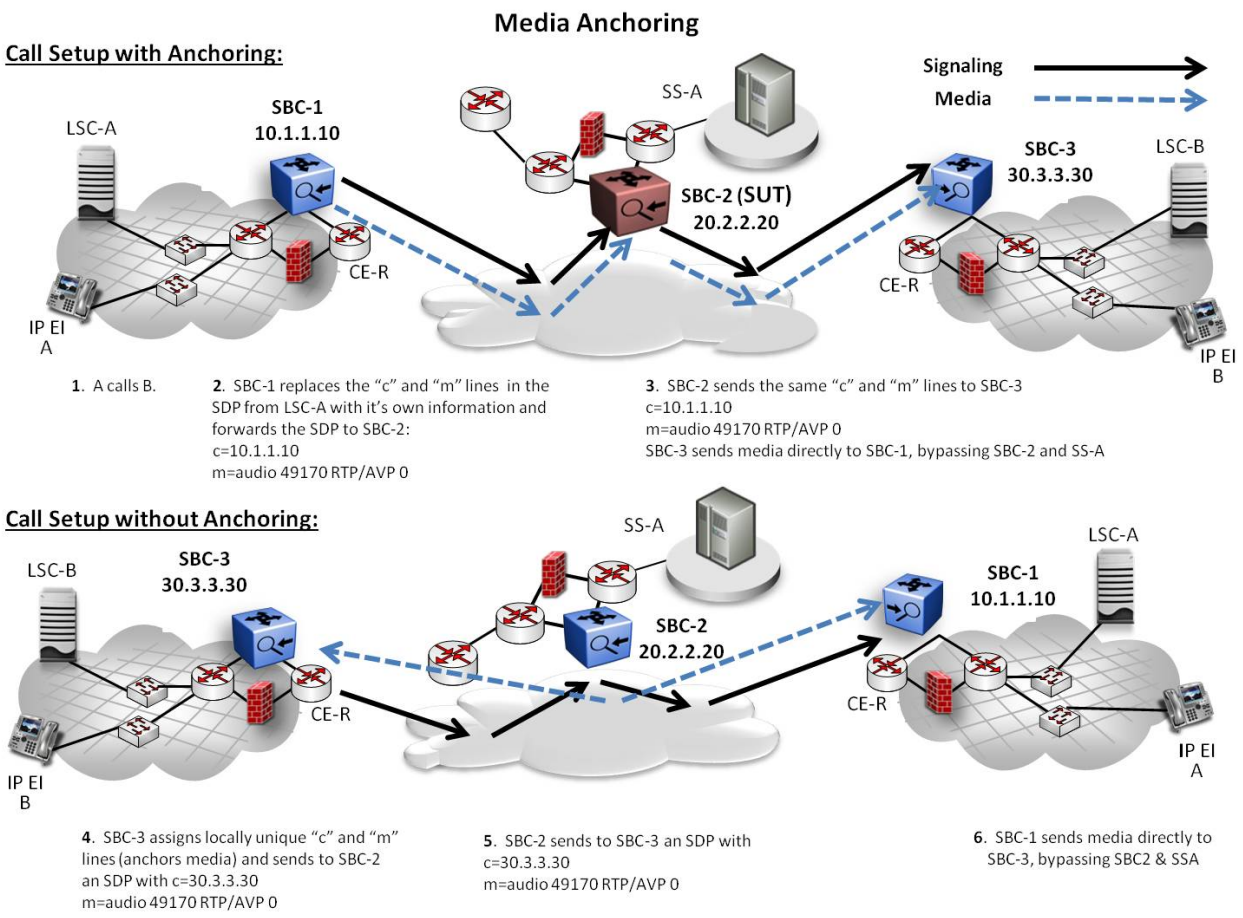


Figure 2. Session Border Controller (SBC) Minimum Test Architecture



Legend:

AVP	Audio-Visual Profile
c	AS-SIP Connection
CE-R	Customer Edge Router
EI	End Instrument
IP	Internet Protocol
LSC	Local Session Controller
NM	Network Management
R	Required
m	Media
RTP	Real Time Protocol
SBC	Session Border Controller
SC	Session Controller
SDP	Session Description Protocol
SS	Softswitch
SUT	System Under Test

Figure 3. Media Anchoring

```
25:31.823 On 200.23.3.4:53274 sent to 200.23.3.241:5061
INVITE sip:3124444641@200.23.3.241:5061;nt_end_pt=nt_server_host=200.23.3.241:5061;cca-
    id=UMFSSFTH01;user=phone;transport=tls SIP/2.0
Via: SIP/2.0/TLS 200.23.3.4:5061;branch=z9hG4bKhp1cj52088ighl8vu1j0sbqhle333.1
From: "3127348910"<sip:3127348910@dsn.mil;user=phone>;tag=gK0c801782
To: "3124444641"<sip:3124444641@dsn.mil;user=phone>;tag=081cf3f3b4e318775533542e900
Call-ID: fd49840054439ca7745ef97515aa82591c812a35@200.23.3.241
CSeq: 978728902 INVITE
Max-Forwards: 69
Allow:
    INVITE,ACK,CANCEL,BYE,REGISTER,REFER,INFO,SUBSCRIBE,NOTIFY,PRACK,UPDATE,OPT
    IONS,MESSAGE,PUBLISH
Accept: application/sdp, application/isup, application/dtmf, application/dtmf-relay,
    multipart/mixed
Contact: <sip:3127348910@200.23.3.4:5061;transport=tls>
Supported: 100rel,replaces
Content-Length: 561
Content-Disposition: session; handling=required
Content-Type: application/sdp

v=0
o=XYZ_SBC_UAC 234190838 2120924235 IN IP4 200.23.3.4
s=SIP Media Capabilities
c=IN IP4 200.23.3.4
t=0 0
m=audio 61606 RTP/SAVP 0 96
a=sqn:0
a=cdsc:1 audio udpsprt 98
a=cpar:a=sprtmap:98 v150mr/8000
a=cpar:a=fmtp:98 mr=1;mg=0;CDSCselect=1;mrmods=1-4,10-14,16-17;jmdelay=no;versn=1.1
a=rtpmap:0 PCMU/8000
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
a=sendrecv
a=crypto:1 AES_CM_128_HMAC_SHA1_32 inline:Ecl3U5/qiudvS28eJ+H37mKo/pK/YbbDq6FF87x3
a=crypto:2 AES_CM_128_HMAC_SHA1_80 inline:Ecl3U5/qiudvS28eJ+H37mKo/pK/YbbDq6FF87x3
a=maxptime:20
```

Figure 4. Example of Contact Header/C and M Anchoring Lines

Table 1 outlines the interfaces specified in the UCR for the SUT. Table 2 outlines the IPv4 interoperability (IO) capability requirements (CRs) and functional requirements (FRs) applicable to the SUT. For UCR IA requirements that are applicable to the component under test, IA testing is performed by the IA team prior to Interoperability (IO) testing. Table 3 outlines the IPv6 interoperability (IO) capability requirements (CRs) and functional requirements (FRs) applicable to the SUT. Test procedure references are denoted as an IO-# throughout this test plan.

Table 1. Interface Requirements

Interface	UCR # /Mark Applicability: (R), (O), (C)	Notes (fill in Interface capability)
Network Management Interfaces		
10BASE-X	R	
100BASE-X	R	
1000BASE-X	C	
Network Interfaces		
10BASE-X	R	
100BASE-X	R	
1000BASE-X	R	
10GBASE-X	O	

LEGEND:

C	Conditional		
CR	Capability Requirement	O	Optional
FR	Functional Requirement	R	Required
GbE	Gigabit Ethernet	UCR	Unified Capabilities Requirements
LAN	Local Area Network	WAN	Wide Area Network

Table 2. Session Border Controller (SBC) Capability/Functional Requirements

CR/FR ID	Requirement	UCR Ref (UCR 2013)	LoC/ TP ID	R/O/C
1	**2.6 Failover and Recovery**			
1-1	Each SC and SBC pairing shall support OPTIONS-based failover by at least one of the following methods: Alternative A: The SC-Generated OPTIONS Method (sec. Section 2.6.1), or Alternative B: The SBC-Generated OPTIONS Method (sec Section 2.6.2). NOTE 1: The SBC is not required to comply with the SBC requirements set forth in Alternative B as long as the SBC complies with the requirements set forth in alternative A. NOTE 2: The SBC that only supports Alternative B MUST be deployed in conjunction with a SC that supports Alternative B.	2.6 SCM-001170	T IO-6 IO-7	R
1-2	The SBC fronting the SC shall send periodic OPTIONS requests to the SBC fronting the primary SS.	2.6.2.1 SCM-001350	T IO-7	R
1-3	The interval between sending OPTIONS requests shall be configurable with a minimum interval of 35 seconds and a default interval of 60 seconds.	2.6.2.1 SCM-001350.a	T IO-7	R
1-4	The SBC fronting the SC shall send periodic OPTIONS requests to the SBC fronting the secondary SS.	2.6.2.1 SCM-001360	T IO-7	R
1-5	The interval between sending OPTIONS requests shall be configurable with a minimum interval of 35 seconds and a default interval of 60 seconds.	2.6.2.1 SCM-001360.a	T IO-7	R
1-6	The SBC fronting the primary SS shall send periodic OPTIONS requests to the primary SS.	2.6.2.1 SCM-001370	T IO-7	R
1-7	The interval between sending OPTIONS requests shall be configurable with a minimum interval of 35 seconds and a default interval of 60 seconds.	2.6.2.1 SCM-001370.a	T IO-7	R
1-8	The SBC fronting the secondary SS shall send periodic OPTIONS requests to the secondary SS.	2.6.2.1 SCM-001380	T IO-7	R
1-9	The interval between sending OPTIONS requests shall be configurable with a minimum interval of 35 seconds and a default interval of 60 seconds.	2.6.2.1 SCM-001380.a	T IO-7	R
1-10	The SBC fronting the SC shall mark the path to the primary SS as unavailable when the SBC fronting the SC sends a configurable number of consecutive OPTIONS requests to the SBC fronting the primary SS to which it either receives no response or receives a response code of 408 (Request Time-Out), 500 (Server Internal Error), 503 (Service Unavailable) or 504 (Server Time-Out).	2.6.2.2 SCM-001390	T IO-7	R
1-11	The default number of consecutive failed OPTIONS requests is 2.	2.6.2.2 SCM-001390.a	T IO-7	R
1-12	The SBC fronting the primary SS shall mark the path to the primary SS as unavailable when the SBC fronting the primary SS sends a configurable number of consecutive OPTIONS requests to the primary SS to which it either receives no response or receives a response code of 408 (Request Time-Out), 500 (Server Internal Error), 503 (Service Unavailable) or 504 (Server Time-Out).	2.6.2.2 SCM-001400	T IO-7	R
1-13	The default number of consecutive failed OPTIONS requests is 2.	2.6.2.2 SCM-001400.a	T IO-7	R
1-14	The SBC fronting the SC shall mark the path to the secondary SS as unavailable when the SBC fronting the SC sends a configurable number of consecutive OPTIONS requests to the SBC fronting the secondary SS to which it either receives no response or receives a 408 (Request Time-Out), 500 (Server Internal Error), 503 (Service Unavailable) or 504 (Server Time-Out).	2.6.2.2 SCM-001410	T IO-7	R
1-15	The default number of consecutive failed OPTIONS requests is 2.	2.6.2.2 SCM-001410.a	T IO-7	R
1-16	The SBC fronting the secondary SS shall mark the path to the secondary SS as unavailable when the SBC fronting the secondary SS sends a configurable number of consecutive OPTIONS requests to the secondary SS to which it either receives no response or receives a 408 (Request Time-Out), 500 (Server Internal Error), 503 (Service Unavailable) or 504 (Server Time-Out).	2.6.2.2 SCM-001420	T IO-7	R
1-17	The default number of consecutive failed OPTIONS requests is 2.	2.6.2.2 SCM-001420.a	T IO-7	R
1-18	When the SBC fronting the SC marks the path to the primary SS as unavailable AND the SBC fronting the SC receives an outbound request from the SC whose Route header(s) identify the next hop to be the SBC serving the primary SS, then the SBC serving the SC shall respond with either a 500 (Server Internal Error), 503 (Service Unavailable) or 504 (Server Time-Out).	2.6.2.2 SCM-001430	T IO-7	R

Table 2. Session Border Controller (SBC) Capability/Functional Requirements (continued)

CR/FR ID	Requirement	UCR Ref (UCR 2013)	LoC/ TP ID	R/O/C
1-19	When the SBC fronting the primary SS marks the path to the primary SS as unavailable AND the SBC fronting the primary SS receives an outbound request from the SBC serving the SC then the SBC serving the primary SS shall respond with either a 500 (Server Internal Error), 503 (Service Unavailable) or 504 (Server Time-Out).	2.6.2.2 SCM-001440	T IO-7	R
1-20	When the SBC fronting the SC marks the path to the secondary SS as unavailable AND the SBC fronting the SC receives an outbound request from the SC whose Route header(s) identify the next hop to be the SBC serving the secondary SS, then the SBC serving the SC shall respond with either a 500 (Server Internal Error), 503 (Service Unavailable) or 504 (Server Time-Out).	2.6.2.2 SCM-001450	T IO-7	R
1-21	When the SBC fronting the secondary SS marks the path to the secondary SS as unavailable AND the SBC fronting the secondary SS receives an outbound request from the SBC serving the SC then the SBC serving the secondary SS shall respond with either a 500 (Server Internal Error), 503 (Service Unavailable) or 504 (Server Time-Out).	2.6.2.2 SCM-001460	T IO-7	R
1-22	When the SBC fronting the SC has marked the path to the primary SS as unavailable then the SBC fronting the SC shall send periodic OPTIONS requests to the SBC fronting the primary SS.	2.6.2.3 SCM-001470	T IO-7	R
1-23	The interval between sending OPTIONS requests shall be configurable with a minimum interval of 35 seconds and a default interval of 60 seconds.	2.6.2.3 SCM-001480	T IO-7	R
1-24	When the SBC fronting the primary SS responds with 200 (OK) to a configurable number of consecutive OPTIONS requests sent by the SBC fronting the SC then the SBC fronting the SC marks the path to the primary SS as available once again.	2.6.2.3 SCM-001490	T IO-7	R
1-25	The default number of successful OPTIONS requests is 2.	2.6.2.3 SCM-001490.a	T IO-7	R
1-26	Upon failback, the SBC fronting the SC shall send periodic OPTIONS requests to the SBC fronting its primary SS whereby the interval between sending OPTIONS requests shall be configurable with a minimum interval of 35 seconds and a default interval of 60 seconds.	2.6.2.3 SCM-001500	T IO-7	R
1-27	When the SBC fronting the primary SS has marked the path to the primary SS as unavailable then the SBC fronting the primary SS shall send periodic OPTIONS requests to the primary SS.	2.6.2.3 SCM-001510	T IO-7	R
1-28	The interval between sending OPTIONS requests shall be configurable with a minimum interval of 35 seconds and a default interval of 60 seconds.	2.6.2.3 SCM-001510.a	T IO-7	R
1-29	When the primary SS responds with 200 (OK) to a configurable number of consecutive OPTIONS requests sent by the SBC fronting the primary SS then the SBC fronting the primary SS marks the path to the primary SS as available once again.	2.6.2.3 SCM-001520	T IO-7	R
1-30	The default number of successful OPTIONS requests is 2.	2.6.2.3 SCM-001520.a	T IO-7	R
1-31	Upon failback, the SBC fronting the primary SS shall send periodic OPTIONS requests to the primary SS whereby the interval between sending OPTIONS requests shall be configurable with a minimum interval of 35 seconds and a default interval of 60 seconds.	2.6.2.3 SCM-001530	T IO-7	R
1-32	When the SBC fronting the SC has marked the path to the secondary SS as unavailable then the SBC fronting the SC shall send periodic OPTIONS requests to the SBC fronting the secondary SS.	2.6.2.3 SCM-001550	T IO-7	R
1-33	The interval between sending OPTIONS requests shall be configurable with a minimum interval of 35 seconds and a default interval of 60 seconds.	2.6.2.3 SCM-001550.a	T IO-7	R
1-34	When the SBC fronting the secondary SS responds with 200 (OK) to a configurable number of consecutive OPTIONS requests sent by the SBC fronting the SC then the SBC fronting the SC marks the path to the secondary SS as available once again.	2.6.2.3 SCM-001560	T IO-7	R
1-35	The default number of successful OPTIONS requests is 2.	2.6.2.3 SCM-001560.a	T IO-7	R
1-36	Upon failback, the SBC fronting the SC shall send periodic OPTIONS requests to the SBC fronting its secondary SS whereby the interval between sending OPTIONS requests shall be configurable with a minimum interval of 35 seconds and a default interval of 60 seconds.	2.6.2.3 SCM-001570	T IO-7	R

Table 2. Session Border Controller (SBC) Capability/Functional Requirements (continued)

CR/FR ID	Requirement	UCR Ref (UCR 2013)	LoC/ TP ID	R/O/C
1-37	When the SBC fronting the secondary SS has marked the path to the secondary SS as unavailable then the SBC fronting the secondary SS shall send periodic OPTIONS requests to the secondary SS.	2.6.2.3 SCM-001580	T IO-6 IO-7 IO-8	R
1-38	The interval between sending OPTIONS requests shall be configurable with a minimum interval of 35 seconds and a default interval of 60 seconds.	2.6.2.3 SCM-001580.a	T IO-7	R
1-39	When the secondary SS responds with 200 (OK) to a configurable number of consecutive OPTIONS requests sent by the SBC fronting the secondary SS then the SBC fronting the secondary SS marks the path to the secondary SS as available once again.	2.6.2.3 SCM-001590	T IO-7	R
1-40	The default number of successful OPTIONS requests is 2.	2.6.2.3 SCM-001590a	T IO-7	R
1-41	Upon failback, the SBC fronting the secondary SS shall send periodic OPTIONS requests to the secondary SS whereby the interval between sending OPTIONS requests shall be configurable with a minimum interval of 35 seconds and a default interval of 60 seconds.	2.6.2.3 SCM-001600	T IO-7	R
2	**2.12.4– Session Border Controller (SBC) deployed within the Enterprise UC Services architecture**			
2-1	Internal interfaces are functions that operate internal to a System Under Test (SUT) or UC-approved product (e.g., SC, SS). The interfaces between SC/SS functions within an SC (e.g., between the Call Admission Control (CAC), Interworking Function (IWF), MGC, and MG) and Signaling Gateway (SG) are considered internal to the SC regardless of the physical packaging. These interfaces are vendor-proprietary and unique, especially the protocol used over the interface. Whenever the physical interfaces use Institute of Electrical and Electronics Engineers, Inc. (IEEE) 802.3 Ethernet standards, they shall support auto-negotiation even when the IEEE 802.3 standard has it as optional. This applies to 10/100/1000-T Ethernet standards; i.e., IEEE, Ethernet Standard 802.3, 1993; or IEEE, Fast Ethernet Standard 802.3u, 1995; and IEEE, Gigabit Ethernet Standard 802.3ab, 1999.	2.7.1 SCM-001770	L/T IO-4	R
2-2	The SC (and its appliances), SS and, SBC shall support 10/100/1000-T Mbps Ethernet physical interfaces to ASLAN switches and routers. Whenever the physical interfaces use IEEE 802.3 Ethernet standards, they shall support auto-negotiation even when the IEEE 802.3 standard has it as optional. This applies to 10/100/1000-T Ethernet standards; i.e., IEEE, Ethernet Standard 802.3, 1993; or IEEE, Fast Ethernet Standard 802.3u, 1995; and IEEE, Gigabit Ethernet Standard 802.3ab, 1999.	2.7.2 SCM-001780	L/T IO-4	R
2-3	The SBC shall support an ASLAN-side 10Base-X Ethernet interface and a WAN-side 10Base-X Ethernet interface.	2.7.2 SCM-001790	L/T IO-4	R
2-4	The SBC shall support 100Base-X Ethernet, or Gigabit Ethernet (Gbe), or 10Gigabit Ethernet (10GbE), full duplex interfaces on both the ASLAN-side and the WAN-side.	2.7.2 SCM-001800	L/T IO-4	O
2-5	SBC shall support a 10/100-Mbps Ethernet physical interface to the DISA VVoIP EMS. The interface will work in either of the two following modes using auto-negotiation: IEEE, Ethernet Standard 802.3, 1993; or IEEE, Fast Ethernet Standard 802.3u, 1995.	2.7.4 SCM-001830	L/T IO-4	R

Table 2. Session Border Controller (SBC) Capability/Functional Requirements (continued)

CR/FR ID	Requirement	UCR Ref (UCR 2013)	LoC/ TP ID	R/O/C
2-6	Local management traffic and VVoIP EMS management traffic shall use separate physical Ethernet interfaces. Redundant VVoIP EMS physical Ethernet interfaces may be used but are not required. Redundant local management physical Ethernet interfaces may be used but are not required. Redundant physical Ethernet interfaces are required for signaling and bearer traffic. If the primary signaling and bearer Ethernet interface fails, then traffic shall be switched to the backup signaling and bearer Ethernet interface. When the primary Ethernet interface fails, the secondary Ethernet interface has to have the same IP address. The failover from the primary to the secondary interface shall comply with the specifications in Section 7.6.6.2, Dual Product Redundancy. Signaling and bearer traffic may use the same physical Ethernet interface as local or VVoIP EMS management traffic, or it may use a separate physical Ethernet interface.	2.7.4 SCM-001840	T IO-4	O
2-7	If signaling and bearer traffic shares a physical Ethernet interface with local or VVoIP EMS management traffic, then the signaling and bearer traffic shall use a separate VLAN.	2.7.4 SCM-001850	T IO-4	C
2-8	The enclave SBC shall send the UCR-compliant voice media packets received from the UC WAN and intended for the IP EIs served by the proprietary UC signaling platform to the AS-SIP IP Gateway.	2.11.2.4 SCM-003820	L	R
2-9	The enclave SBC shall send the UCR-compliant video media packets received from the UC WAN and intended for the IP EIs served by the proprietary UC signaling platform to the AS-SIP IP Gateway.	2.11.2.4 SCM-003850	L	R
2-10	The enclave SBC shall send the UCR-compliant voice media packets received from the UC WAN and intended for the IP EIs served by the H.323 UC signaling platform to the AS-SIP – H.323 Gateway.	2.11.3.7 SCM-004150	L	R
2-11	The enclave SBC shall send the UCR-compliant video media packets received from the UC WAN and intended for the IP EIs served by the H.323 UC signaling platform to the AS-SIP – H.323 Gateway.	2.11.3.7 SCM-004180	L	R
2-12	SBCs deployed within the Enterprise UC Services architecture shall support SBC functionality defined in this section (subject to the modifications and additions set forth in this subsection).	2.12.4.1 SCM-005610	N/A	R
2-13	The enclave-fronting SBC shall be able to differentiate an intra-enclave VVoIP sessions from an inter-enclave VVoIP sessions. For inter-enclave VVoIP sessions routed through the enclave-fronting SBC, the enclave-fronting SBC shall perform the bidirectional anchoring of the associated media as defined in this section. For all intra-enclave VVoIP sessions, the enclave-fronting SBC shall not perform the bidirectional anchoring of the associated media.	2.12.4.2 SCM-005620	T IO-5	R
2-14	The ESC APL SUT shall offer Enclave-Fronting SBC solutions that meet High Available SBC or Medium Available SBC requirements as defined in this section.	2.12.4.2 SCM-005630	L	R
2-15	The Enclave-Fronting SBC solution deployed at an Environment 1 location shall meet High Available SBC requirements defined in this section.	2.12.4.2 SCM-005640	L	R
2-16	The Enclave-Fronting SBC solution deployed at an Environment 2 or 3 location may comply with Medium Available SBC requirements as defined in this section	2.12.4.2 SCM-005650	L	O
2-17	To enable full topology hiding [Network Address Translation (NAT)] of signaling and bearer traffic, the enclave-fronting SBC shall function as the outbound and inbound signaling proxy for all AS-SIP signaling traffic exchanged between AEIs and the centralized ESC.	2.12.4.2.1 SCM-005660	L/T IO-5	R
2-18	For the routing of AS-SIP signaling traffic exchanged between AEIs and the centralized ESC, the enclave-fronting SBC shall be capable of maintaining a persistent TLS connection with every served AEI within the enclave and the ESC-fronting SBC.	2.12.4.2.1 SCM-005670	L/T IO-5	R

Table 2. Session Border Controller (SBC) Capability/Functional Requirements (continued)

CR/FR ID	Requirement	UCR Ref (UCR 2013)	LoC/ TP ID	R/O/C
2-19	The enclave-fronting SBC shall function as a registration proxy for all AEIs located within the associated enclave: a. When a served AEI sends an AS-SIP REGISTER request to the enclave-fronting SBC, the enclave-fronting SBC shall replace the IP address and port value contained in the Contact header of the REGISTER message (i.e., the inside-address/port) with an IP address and port value associated with a WAN-facing interface on the enclave-fronting SBC (i.e., the outside-address/port).	2.12.4.2.1 SCM-005680	L/T IO-5	R
2-20	If served PEIs are relying upon the enclave-fronting SBC to facilitate the traversal of the enclave IA accreditation boundary, the enclave-fronting SBC shall function as a VVoIP aware firewall for vendor-proprietary signaling exchanged between PEIs and the centralized ESC. The enclave-fronting SBC shall maintain a secure, persistent connection (TLS or equivalent) with each served PEI within the enclave and with the ESC-fronting SBC within the ESC Core Infrastructure.	2.12.4.2.2 SCM-005690	L/T IO-5	C
2-21	If served PEIs are relying upon the enclave-fronting SBC to facilitate the traversal of the enclave IA accreditation boundary, the enclave-fronting SBC shall function as a Application-Layer Gateway (ALG) capable of performing the bidirectional mapping of embedded inside-addresses/port values (within the signaling stream) to an outside-address/port value associated with a WAN-facing interface on the enclave-fronting SBC.	2.12.4.2.2 SCM-005700	L/T IO-12	C
2-22	For the routing of AS-SIP signaling exchanged between AEIs and the centralized ESC, the ESC-fronting SBC shall maintain a persistent TLS connection with the ESC and with the enclave-fronting SBC at each AEI-hosting enclave within the ESA.	2.12.4.3 SCM-005710	L/T IO-12	R
2-23	If served PEIs are relying upon the ESC-fronting SBC to facilitate the traversal of the ESC Core IA accreditation boundary, the ESC-fronting SBC shall maintain a secure, persistent connection (TLS or equivalent) with the centralized ESC and the enclave-fronting SBC at each PEI-hosting enclave within the ESA.	2.12.4.3 SCM-005720	L/T IO-12	C
	The ESC-fronting SBC shall perform media anchoring on media streams to or from Enterprise media resources which are co-located with the ESC (e.g., an Enterprise conference bridge or an announcement server).	2.12.4.3 SCM-005730	L/T IO-12	R
2-24	With the exception of media streams to or from media resources co-located with the ESC (e.g., an Enterprise conference bridge or an announcement server), the ESC-fronting SBC shall NOT conduct media anchoring.	2.12.4.3 SCM-005740	L/T IO-12	R
2-25	The ESC-fronting SBC shall be a High Available SBC as defined in this section.	2.12.4.3 SCM-005750	L	R
3	**2.16-Remote Media Gateway**			
3-1	If an MG is geographically separated from the MGC that controls it, then the following five specific conditional requirements address the SBC, the MG control protocol, the DSCP for the control packets, and the security aspects for that arrangement.	2.16.13 SCM-008430	NA	C
3-2	The SRTP media stream and the H.248.1 control packets shall pass through an SBC deployed as part of the Remote MG SUT. The H.248.1 protocol uses well known UDP ports: MG port 2727 and MGC port 2427. Within the IPSec channel, these two ports shall be left open by the SBC, which shall allow only authenticated SCs and SSs to access these port numbers. The requirements for the SBC are given in Section 2.17.10, SBC Requirements to Support Remote MG.	2.16.13 SCM-008440	L	C

Table 2. Session Border Controller (SBC) Capability/Functional Requirements (continued)

CR/FR ID	Requirement	UCR Ref (UCR 2013)	LoC/ TP ID	R/O/C
3-3	The IP Sec with H.248.1 shall be used on the MGC to MGC SBC channel, the MGC SBC to remote MG SBC channel, and on the remote MG SBC to Remote MG channel to secure the MG control protocol packets as specified in Section 4.2.5, Confidentiality [Internet Key Exchange (IKE) version 1, Advanced Encryption Standard (AES) 128, Oakley Group 2048 support, etc.]. Multiple Remote MGs can be controlled by a single MGC. A single IPSec channel shall be used between the MGC and the MGC SBC to encapsulate the multiple H.248.1 control streams. The MGC SBC shall establish separate IPSec channels to each of the Remote MG SBCs, and use the H.248.1 packet header IP address information to route the H.248.1 packets (modified by NAT if it is used) to the corresponding IPSec channel to each of the remote MG SBCs. The Remote MG SBC shall unencapsulate the IPSec channel, use the control information to open and close media stream pinholes, apply NAT if used, and reencapsulate the H.248.1 packets into the IPSec channel to the MG.	2.16.13 SCM-008480	L	C
4	**2.17-Session Border Controller (SBC)**			
4-1	The SBC shall present one or more signaling IP addresses to each network side (one to the LAN [red] side and one to the network [black] side). The SBC shall also present one or more media IP addresses to each network side (one to the LAN [red] side and one to the network [black] side). In both the signaling and media cases, each individual IP address shall be implemented in the SBC as either a single logical IP address or a single physical IP address.	2.17 SCM-008490	L/T IO-6 IO-7	R
4-2	The SBC shall still meet all of the VVoIP Intrusion Detection System (IDS) monitoring requirements in this configuration (multiple signaling IP address and multiple media IP addresses on each network side). The SBC IDS monitoring requirements are in Section 4.2.3.4, Ancillary Equipment. The functionality that each VVoIP IDS/Intrusion Prevention System (IPS) shall provide is specified in Section 13.2.4, IPS Functionality, and Section 13.2.5, IPS VVoIP Signal and Media Inspection.	2.17 SCM-008500 Info Only. See Errata 2	L	R
4-3	The product shall act as an AS-SIP B2BUA for interpreting the AS-SIP messages to meet its functions.	2.17.1 SCM-008510	T IO-5	R
4-4	The product shall be capable of bidirectional anchoring (NAT and NAPT) the media associated with a voice or video session that originates or terminates within its enclave.	2.17.1 SCM-008520	T IO-5	R
4-5	The product shall assign a locally unique combination of “c” and “m” lines when anchoring the media stream.	2.17.1 SCM-008520.A	T IO-5	R
4-6	If an INVITE request is forwarded to a product fronting an SS for which the INVITE request is not destined (i.e., the SS will forward the INVITE request downstream to another SS or SC), the product shall be capable of anchoring the media upon receipt of the INVITE request, but shall restore the original “c” and “m” lines upon receipt of the forwarded INVITE request from the SS.	2.17.1 SCM-008520.B	T IO-5	R
4-7	If a session is forwarded or transferred so the session is external to the enclave (i.e., the session no longer terminates or originates within the enclave), then the product shall restore the original received “c” and “m” lines to the Forwarding/transfer message, as appropriate, to ensure that the media is no longer anchored to that product.	2.17.1 SCM-008520.C	T IO-5	R
4-8	The SBC shall be capable of processing Route headers IAW RFC 3261, Sections 20.34, 8.1.2, 16.4, and 16.12.	2.17.1 SCM-008530	T IO-5	R
4-9	The product shall preserve/pass the CCA-ID field in the Contact header.	2.17.1 SCM-008560	T IO-5	R
4-10	The product shall always decrement the Max-Forward header.	2.17.1 SCM-008570	T IO-5	R
4-11	The product shall modify the Contact header to reflect its IP address to ensure it is in the return routing path.	2.17.1 SCM-008580	T IO-5	R
4-12	The product fronting an SC shall be capable of maintaining a persistent TLS session between the SBC fronting the primary SS and the SBC fronting the secondary SS. Persistent means the TLS session is established when the product joins the signaling network, and it is not established on a session-by-session basis.	2.17.1 SCM-008590	T IO-5	R

Table 2. Session Border Controller (SBC) Capability/Functional Requirements (continued)

CR/FR ID	Requirement	UCR Ref (UCR 2013)	LoC/ TP ID	R/O/C
4-13	The SBC shall be capable of distinguishing between the primary (associated with the primary SS) and a secondary (associated with the secondary SS) TLS path for the purposes of forwarding AS-SIP messages.	2.17.1 SCM-008590.a	T IO-6 IO-7	R
4-14	The SBC initiates a session toward its fronted SC/SS (arriving from the WAN) when receiving an incoming INVITE AS-SIP message from the WAN.	2.17.1 SCM-008590.b	T IO-6 IO-7	R
4-15	The product shall be capable of handling the aggregated WAN call processing load associated with its SCs and SSs.	2.17.2 SCM-008600	L	R
4-16	The product shall support FCAPS Network Management functions as defined in Section 2.19, Management of Network Appliances, of this document.	2.17.3 SCM-008610	L	R
4-17	The SBC shall ensure that media streams associated with a particular session use the appropriate DSCP based on the information in the AS-SIP RPH.	2.17.4 SCM-008620	T IO-1	O
4-18	Packets that are not marked with the appropriate DSCP shall be dropped.	2.17.4 SCM-008630	T IO-1	O
4-19	The SBC shall perform this policing for media packets received from the ASLAN that are destined for points outside of the ASLAN, and for media packets received from the WAN that are destined for points within the ASLAN.	2.17.4 SCM-008640	T IO-1	O
4-20	The SBC shall be capable of ensuring that the media streams associated with a particular session use the appropriate codec (bandwidth) based on the SDP information in the AS-SIP message. The SBC is allowed to drop any session with an associated media stream that exceeds the negotiated bandwidth, or it may perform traffic shaping on the offending media stream.	2.17.5 SCM-008650	L	O
4-21	The product shall have an availability of 99.999 percent (non-availability of no more than 5 minutes per year). The product shall meet the requirements specified in Section 2.8.2, Product Quality Factors, of this document. See SCM-001860-SCM-1900 for requirements.	2.17.6 SCM-008660	L/T IO-9 IO-10 IO-11	R
4-22	The product shall have an availability of 99.99 percent. The product shall meet the requirements specified in Section 2.8.2.1, Product Availability, except for Item i, No Loss of Active Sessions. See SCM-001860-SCM-1900 for requirements.	2.17.6 SCM-008670	L/T IO-9 IO-10 IO-11	R
4-23	The product shall be capable of supporting the IEEE 802.1Q 2-byte TCI Field 12-bit Virtual Local Area Network Identification (VID).	2.17.7 SCM-008680	L/T IO-3	R
4-24	The product shall be capable of receiving, processing, and transmitting a UC packet within 2 ms to include executing all internal functions.	2.17.8 SCM-008690	T IO-5	R
4-25	If the SBC supports H.323 video, then the product shall be capable of processing and forwarding H.323 messages IAW Section 4, Information Assurance.	2.17.9 SCM-008700	L	C
4-26	If an MG is geographically separated from the MGC that controls it, then the media stream encapsulated in SRTP, and the H.248.1 control packets encapsulated with IPSec shall pass through an SBC deployed as part of the Remote MG SUT. Within the IPSec channel, the H.248.1 protocol uses well-known UDP ports: MG port 2727 and MGC port 2427. The MG SBC shall act as an Application Layer Gateway on H.248.1 sessions, in the same manner as it acts as a B2BUA on AS-SIP sessions, to open and close pinholes for authorized and authenticated bearer sessions.	2.17.10 SCM-008710	L	C
4-27	The product shall support more than one SC.	2.17.11 SCM-008720	L	O

Table 2. Session Border Controller (SBC) Capability/Functional Requirements (continued)

CR/FR ID	Requirement	UCR Ref (UCR 2013)	LoC/ TP ID	R/O/C
5-1	There shall be a local craftsperson interface [Craft Input Terminal (CIT)] for OAM&P for all VVoIP appliances. The CIT is a supplier-provided input/output device that is locally connected to a network component. The CIT may be connected to the local EMS, which is in turn connected to the VVoIP appliance using the local EMS Ethernet management interface. The CIT may be connected directly to the VVoIP appliance also, using the Ethernet management interface on the component that would otherwise be used by the local EMS (when there is no local EMS). The CIT may be connected directly to the VVoIP appliance using a separate serial interface	2.19.1 SCM-009120	L	R
5-2	Communications between VVoIP EMS and the VVoIP appliances shall be via IP.	2.19.1 SCM-009130	L	R
5-3	Network appliance shall issue state change notifications for changes in the states of replaceable components, including changes in operational state or service status, and detection of new components.	2.19.1 SCM-009150	L	R
5-4	A network appliance shall be provisioned by the VVoIP EMS with the address and Transport Layer port information associated with its Core Network interfaces.	2.19.1 SCM-009160	L	R
5-5	A network appliance shall be capable of maintaining and responding to VVoIP EMS requests for resource inventory, configuration, and status information concerning Core Network interface resources (e.g., IP or MAC addresses) that have been installed and placed into service.	2.19.1 SCM-009170	L	R
5-6	A network appliance shall be capable of setting the Administrative state and maintaining the Operational state of each Core Network interface and maintaining the time of the last state change.	2.19.1 SCM-009180	L	R
5-7	A network appliance shall generate an alarm condition upon the occurrence of any of the following failure conditions, as defined in ITU-T Recommendation M.3100: A network appliance shall generate an alarm condition upon the occurrence of power loss.	2.19.1 SCM-009190 SCM-09190.A	L	R
5-8	A network appliance shall generate an alarm condition upon the occurrence of any of the following failure conditions, as defined in ITU-T Recommendation M.3100: Environmental condition not conductive to normal operation.	2.19.1 SCM-009190 SCM-09190.B	L	R
5-9	A network appliance shall generate an alarm condition upon the occurrence of any of the following failure conditions, as defined in ITU-T Recommendation M.3100: Loss of data integrity.	2.19.1 SCM-009190 SCM-009190.C	L	R
5-10	A network appliance shall generate an alarm condition when the number of received packets that fail encoding integrity checks exceeds a configurable threshold.	2.19.1 SCM-009200	L	R
5-11	A network appliance shall generate an alarm condition when the number of received packets that fail decryption exceeds a configurable threshold.	2.19.1 SCM-009210	L	R
5-12	A network appliance shall be capable of maintaining and responding to requests for physical resource capacity information for installed components. This information includes the following: a. Component type and model. b. Shelf location. c. Rack location. d. Bay location.	2.19.1 SCM-009220	L	R
5-13	Faults shall be reported IAW IETF RFC 3418.	2.19.2 SCM-009230	L	R
5-14	Alarm messages shall be distinguishable from administrative log messages.	2.19.2 SCM-009240	L	R
5-15	The appliances shall detect their own fault (alarm) conditions.	2.19.2 SCM-009250	L	R
5-16	The NEs shall generate alarm notifications	2.19.2 SCM-009260	L	R

Table 2. Session Border Controller (SBC) Capability/Functional Requirements (continued)

CR/FR ID	Requirement	UCR Ref (UCR 2013)	LoC/ TP ID	R/O/C
5-17	The network elements shall send the alarm messages in near-real time (NRT). More than 99.95 percent of alarms shall be detected and reported in NRT. NRT is defined as event detection and alarm reporting within 5 seconds of the event, excluding transport time.	2.19.2 SCM-009270	L	R
5-18	The network components shall send alarm messages in Simple Network Management Protocol (SNMP) version 3 (SNMPv3) format.	2.19.2 SCM-009280	L	R
	All Configuration Management (CM) information shall be presented IAW RFC 3418.	2.19.2 SCM-009290	L	O
5-19	Capability to access and modify configuration data by the VVoIP EMS shall be controllable by using an access privileges function within the network appliance.	2.19.2 SCM-009300	L	R
5-20	Performance Management (PM) information shall be presented IAW RFC 3418.	2.19.2.4 SCM-009430	L	O
5-21	Security Management: All network management interactions shall meet the access control, confidentiality, integrity, availability, and non-repudiation requirements in Section 4, Information Assurance.	2.19.2.5 SCM-009580	L	R
6	**2.2 Voice Features and Capabilities[1]**			
6-1	The Assured Services product's support for these vendor-proprietary VVoIP features and capabilities shall not adversely affect the required operation of the MLPP or ASAC features on that product. The required operation of the MLPP and ASAC features is specified in Section 2.25.1, MLPP; this section; and AS-SIP 2013. In addition, vendor-proprietary VVoIP features and capabilities on Assured Services products shall work with and interact with these MLPP and ASAC features, so that all the UCR requirements for MLPP and ASAC are still met. A vendor-proprietary VVoIP feature or capability shall not cause the MLPP feature to fail, and it shall not cause the ASAC feature to fail.	2.2 SCM-000010	T IO-2 IO-2a IO-2b IO-2c IO-2d IO-2e IO-2f	R
6-2	If a call forwarding feature that does not support interaction with MLPP is activated or configured for a given DN, incoming calls to that DN at PRIORITY or above precedence shall not be forwarded, and shall be processed as if the call forwarding feature is not active or configured.	2.2.1 SCM-000020	T IO-2 IO-2a IO-2b IO-2c	C
6-3	Reminder Ring for all call forwarding features, as specified in accordance with (IAW) Telcordia Technologies GR-217-CORE, GR-580-CORE, and GR-586-CORE, shall be supported. The UC requirements for Reminder Ring are optional.	2.2.1 SCM-000030	T IO-2 IO-2a IO-2b IO-2c	O
6-4	CFV shall be supported IAW Telcordia Technologies GR-580-CORE.	2.2.1.1 SCM-000040	T IO-2 IO-2a	R
6-5	CFV shall interact with MLPP IAW Section 2.2.2.1, Call Forwarding at a Busy Station.	2.2.1.1 SCM-000050	T IO-2 IO-2a	O
6-6	CFBL shall be supported IAW Telcordia Technologies GR-586-CORE.	2.2.1.2 SCM-000060	T IO-2 IO-2b	R
6-7	CFBL shall interact with MLPP IAW Section 2.2.2.1, Call Forwarding at a Busy Station.	2.2.1.2 SCM-000070	T T IO-2 IO-2b	
6-8	CFDA shall be supported IAW Telcordia Technologies GR-586-CORE.	2.2.1.3 SCM-000080	T IO-2 IO-2c	R
6-9	CFDA shall interact with MLPP IAW Section 2.2.2.1, Call Forwarding at a Busy Station, and Section 2.2.2.2, Call Forwarding – No Reply at Called Station.	2.2.1.3 SCM-000090	T IO-2 IO-2c	O
6-10	If SCF is supported, it shall be provided IAW Telcordia Technologies GR-217-CORE.	2.2.1.4 SCM-000100	T N/A	C

Table 2. Session Border Controller (SBC) Capability/Functional Requirements (continued)

CR/FR ID	Requirement	UCR Ref (UCR 2013)	LoC/ TP ID	R/O/C
6-11	SCF shall interact with MLPP IAW Section 2.2.2.1, Call Forwarding at a Busy Station, and Section 2.2.2.2, Call Forwarding – No Reply at Called Station.	2.2.1.4 SCM-000110	T N/A	O
6-12	If a call is forwarded by a CF feature that supports MLPP, the precedence level of the call shall be preserved during the forwarding process.	2.2.2 SCM-000120	T IO-2 IO-2a IO-2b IO-2c	C
	If a called DN has a CF feature active or configured that supports MLPP: • If the incoming call is of a higher precedence level than the established call (or calls, if Three-Way Calling (TWC) is established) at the busy DN being called, then all calls to the busy DN shall be preempted and the incoming call shall be established, i.e., the CF feature shall not be invoked. • If the incoming call is of an equal or lower precedence level than the established call (or calls, if TWC is established) at a busy DN being called, then the CF feature shall be invoked. • If the called IMMEDIATE/PRIORITY (I/P) user, FLASH/FLASH OVERRIDE (F/FO) user, or other UC user is non-preemptable (i.e., is not classmarked for preemption), then the CF feature shall be invoked regardless of the precedence levels of incoming calls and established calls. • The precedence level of calls shall be preserved during the forwarding process. • If the CFBL feature is activated and a precedence call (i.e., PRIORITY and above) is forwarded (including possible multiple forwarding), and if this forwarded call is not responded to by any forwarded-to party within a specified period (e.g., 30 seconds), then the call shall be diverted to an attendant.	2.2.2.1 SCM-000130	T IO-2 IO-2a IO-2b IO-2c IO-2f	C
6-13	If a called DN has a CF feature active or configured that supports MLPP, then the precedence level of calls shall be preserved during the forwarding process, and the forwarded-to user may be preempted.	2.2.2.2 SCM-000140	T IO-2 IO-2a IO-2b IO-2c	C
6-14	If a called DN has a CF feature active or configured that supports MLPP and if a precedence call (i.e., PRIORITY and above) is forwarded (including possible multiple forwarding) and is not responded to by any forwarded-to party (e.g., called party busy with a call of equal or higher precedence level, or called party busy and non-preemptable) within a specified period (e.g., 30 seconds), then the call shall be diverted to an attendant.	2.2.2.2 SCM-000150	T IO-2 IO-2a IO-2b IO-2c	C
6-15	The following Precedence Call Waiting (CW) treatment shall apply to precedence levels of PRIORITY and above.	2.2.3 SCM-000160	T IO-2 IO-2d	R
6-16	If the precedence level of the incoming call is lower than the existing MLPP call, Precedence CW shall be invoked. If the incoming call is PRIORITY precedence or above, the Precedence CW tone (see Table 2.9-2, UC Information Signals) shall be applied to the called party.	2.2.3.1 SCM-000170	T IO-2 IO-2d	R
6-17	The End Instrument (EI) shall provide the Precedence CW tone (see Table 2.9-2, UC Information Signals) to the called user. The EI shall apply this tone regardless of other programmed features, such as CF on busy or caller ID. The called EI shall be able to place the current active call on hold, or disconnect the current active call and answer the incoming call.	2.2.3.2 SCM-000180	T IO-2 IO-2d	R
6-18	Deleted per errata 1	2.2.3.3 SCM-000190	T N/A	R
6-19	If, after receiving the Precedence CW signal, the busy called EI does not answer the incoming UC call within the maximum programmed time interval, then the SC/SS shall treat the call IAW Section 2.2.10, Precedence Call Diversion.	2.2.3.4 SCM-000200	T IO-2 IO-2d	R

Table 2. Session Border Controller (SBC) Capability/Functional Requirements (continued)

CR/FR ID	Requirement	UCR Ref (UCR 2013)	LoC/ TP ID	R/O/C
6-20	Precedence calls arriving at a busy EI that is classmarked as preemptable shall preempt the active lower precedence call. The active busy EI shall receive a continuous preemption tone until an "on-hook" signal is received and the other party shall receive a preemption tone for a minimum of 3 seconds (see Table 2.9-2, UC Information Signals). After going "on-hook," the station to which the precedence call is directed shall be provided precedence ringing (see Table 2.9.1, UC Ringing Tones and Cadences). The station shall be connected to the preempting call after going "off-hook." If CW is enabled on the terminating DN, it shall not be invoked and the existing lower precedence call shall be preempted.	2.2.3.5 SCM-000210	T IO-2 IO-2d	R
6-21	Two types of call transfers are normal and explicit. A normal call transfer is a transfer of an incoming call to another party. An explicit call transfer happens when both calls are originated by the same subscriber. The UC signaling appliance shall provide the interactions described in the following paragraphs, with both normal and explicit call transfers.	2.2.4 SCM-000220	T IO-2 IO-2e	R
6-22	When a call transfer is made at different precedence levels, the SC/SS that initiates the transfer shall classmark the connection at the highest precedence level of the two segments of the transfer.	2.2.4.1 SCM-000230	T IO-2 IO-2e	R
	The SC/SS that initiates a call transfer between two segments that have the same precedence level shall maintain the precedence level upon transfer.	2.2.4.2 SCM-000240	T IO-2 IO-2e	R
6-23	Call Hold is a function of the serving UC signaling appliance system and shall be invoked by going "on-hook," then "off-hook." Calls on hold shall retain the precedence of the originating call.	2.2.5 SCM-000250	T IO-2 IO-2a	R
6-24	In TWC, each call shall have its own precedence level. When a three-way conversation is established, each connection shall maintain its assigned precedence level. Each connection of a call resulting from a split operation shall maintain the precedence level that it was assigned upon being added to the three-way conversation.	2.2.6 SCM-000260	T IO-2 IO-2f	R
6-25	The SC/SS shall classmark the originator of the three-way call at the highest precedence level of the two segments of the call. Incoming calls to lines participating in TWC that have a higher precedence than the higher of the two segments shall preempt unless the call is marked non-preemptable.	2.2.6 SCM-000270	T IO-2 IO-2f	R
6-26	When a higher precedence call is placed to any one of the three-way call participants (including the originator), that participant shall receive the preemption tone (see Table 2.9-2, UC Information Signals). The other two parties shall receive a conference disconnect tone as described in Table 2.9-2. This tone indicates to the other parties that one of the other three-way call participants is being preempted.	2.2.6 SCM-000280	T IO-2 IO-2f	R
6-27	When the originator of the three-way call is on an AEI and is being preempted, the other two parties shall be disconnected from the three-way call.	2.2.6 SCM-000290	T IO-2 IO-2f	R
6-28	When the originator of the three-way call is on a PEI and is being preempted, if the TWC bridge is provided by the PEI, the other two parties shall be disconnected from the three-way call.	2.2.6 SCM-000300	T IO-2 IO-2f	C
6-29	When the originator of the three-way call is on a PEI and is being preempted, if the TWC bridge is provided by the SC or a Media Server, then the other two parties shall remain connected.	2.2.6 SCM-000310	T IO-2 IO-2f	C, O

(Legend on next page)

Table 2. Session Border Controller (SBC) Capability/Functional Requirements (continued)

NOTE:
While Features and Capabilities (UCR Section 2.2) requirements are not specifically labeled as requirements for the SBC, UCR 2013, Errata 1, Section 2.2 states: "It is expected that all Assured Services products, such as SCs and SSs, will support vendor-proprietary VVoIP features and capabilities, in addition to supporting the required VVoIP features and capabilities that are listed in Table 2.2-1, Assured Services Product Features and Capabilities." Through testing, it has been noted that the SBC plays an important role in the in the functioning of call hold, transfers, forwards, and three-way calls. Thus, Features and Capabilities Requirements are listed in this table and are tested in IO-2 to IO-2f procedures.

LEGEND:

AMI	Alternate Mark Inversion
AS	Assured Services
AS	Assured Services Session Initiation Protocol
B8ZS	Bipolar with Eight-Zero Substitution
C	Conditional
CIF	Common Intermediate Format
CORBA	Common Object Request Broker Architecture
CPE	Customer Premise Equipment
CTU	Conferencing Terminal Unit
DCE	Data Circuit-Terminating Equipment
DNIS	Dialed Number Identification Service
DNS	Domain Name Service
DoD	Department of Defense
DSCP	Differentiated Services Code Point
DSN	Defense Switched Network
DTE	Data Terminating Equipment
DTMF	Dual Tone Multi Frequency
EI	End Instrument
EIA	Electronic Industries Alliance
EMS	Element Management System
ESF	Extended Super Frame
FCC	Federal Communications Commission
FECC	Far End Camera Control
FTR	Federal Telecommunications Recommendation
GR	Generic Requirement
ID	Identification
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISDN	Integrated Services Digital Network
ITU	International Telecommunication Union
L	LoC Item
LoC	Letter(s) of Compliance
LSSGR	Local Access and Transport Area (LATA) Switching Systems Generic Requirements
Mbps	Megabits per second
MLPP	Multi-level Precedence and Preemption
MOS	Mean Opinion Score
MTU	Maximum Transmission Unit
NA/SS	Network Appliance/Simple Server
NFAS	Non-Facility Associated Signaling
PKI	Public Key Infrastructure
PRI	Primary Rate Interface
PSTN	Public Switched Telephone Network
QCIF	Quarter Common Intermediate Format
QoS	Quality of Services
R	Required
STIG	Security Technical Implementation Guidelines
SVGA	Super Video Graphics Array
SQCIF	Sub-Quarter Common Intermediate Format
TIA	Telecommunications Industry Association
TP	Test Plan
UC	Unified Capabilities
UCCS	UC Conference System
UCR	Unified Capabilities Requirements
VGA	Video Graphics Array
VTC	Video Teleconferencing
WSXGA+	Widescreen Super Extended Graphics Array Plus

Table 3. IPv6 Requirements

ID	Requirement	UCR 2013 Ref	LoC/ TP ID	R/O/C
IP6-1	**5.2.1 – Product**			
IP6-1-1	The product shall support dual IPv4 and IPv6 stacks described in RFC 4213	5.2.1 IP6-000010	L	R
IP6-1-2	Dual-stack end points or Call Connection Agents (CCAs) shall be configured to choose IPv4 over IPv6.	5.2.1 IP6-000020	L/T IO-2 IO-3	R
IP6-1-3	All nodes and interfaces that are "IPv6- capable" must be carefully configured and verified that the IPv6 stack is disabled until it is deliberately enabled as part of a deliberate transition strategy. This includes the stateless autoconfiguration of link-local addresses. Nodes with multiple network interfaces may need to be separately configured per interface.	5.2.1 IP6-000030	L	R
IP6-1-4	The system shall provide the same (or equivalent) functionality in IPv6 as in IPv4 consistent with the requirements in the UCR for its Approved Products List (APL) category.	5.2.1 IP6-000050	L	R
IP6-1-5	The product shall support the IPv6 format as described in RFC 2460 and updated by RFC 5095.	5.2.1 IP6-000060	L	R
IP6-1-6	The product shall support the transmission of IPv6 packets over Ethernet networks using the frame format defined in RFC 2464.	5.2.1 IP6-000070	L	R
IP6-2	**5.2.1.1 – Maximum Transmission Unit**			
IP6-2-1	The product shall support a minimum MTU of 1280 bytes as described in RFC 2460 and updated by RFC 5095.	5.2.1.1 IP6-000090	L	R
IP6-2-2	If Path MTU Discovery is used and a "Packet Too Big" message is received requesting a next-hop MTU that is less than the IPv6 minimum link MTU, then the product shall ignore the request for the smaller MTU and shall include a fragment header in the packet.	5.2.1.1 IP6-000100	L	C
IP6-3	**5.2.1.2 – Flow Label**			
IP6-3-1	The product shall not use the Flow Label field as described in RFC 2460.	5.2.1.2 IP6-000110	L	R
IP6-3-2	The product shall be capable of setting the Flow Label field to zero when originating a packet.	5.2.1.2 IP6-000120	L	R
IP6-3-4	The product shall be capable of ignoring the Flow Label field when receiving packets.	5.2.1.2 IP6-000140	L	R
IP6-4	**5.2.1.3 – Address**			
IP6-4-1	The product shall support the IPv6 Addressing Architecture as described in RFC 4291.	5.2.1.3 IP6-000150	L	R
IP6-4-2	The product shall support the IPv6 Scoped Address Architecture as described in RFC 4007.	5.2.1.3 IP6-000160	L	R
IP6-4-3	If a scoped address (RFC 4007) is used, then the product shall use a scope index value of zero when the default zone is intended.	5.2.1.3 IP6-000170	L	C
IP6-5	**5.2.1.5 – Neighbor Discovery**			
IP6-5-1	The product shall support Neighbor Discovery for IPv6 as described in RFC 4861.	5.2.1.5 IP6-000280	L	R
IP6-5-2	The product shall not set the override flag bit in the Neighbor Advertisement message for solicited advertisements for any cast addresses or solicited proxy advertisements.	5.2.1.5 IP6-000300	L	R
IP6-5-3	When a valid "Neighbor Advertisement" message is received by the product and the product neighbor cache does not contain the target's entry, the advertisement shall be silently discarded.	5.2.1.5 IP6-000310	L	R
IP6-5-4	When a valid "Neighbor Advertisement" message is received by the product and the product neighbor cache entry is in the INCOMPLETE state when the advertisement is received and the link layer has addresses and no target link-layer option is included, the product shall silently discard the received advertisement.	5.2.1.5 IP6-000320	L	R
IP6-5-5	When address resolution fails on a neighboring address, the entry shall be deleted from the product's neighbor cache.	5.2.1.5 IP6-000330	L	R
IP6-5-6	The product shall support the ability to configure the product to ignore Redirect messages.	5.2.1.5.1 IP6-000340	L	R
IP6-5-7	The product shall only accept Redirect messages from the same router as is currently being used for that destination.	5.2.1.5.1 IP6-000350	L	R

Table 3. IPv6 Requirements (continued)

ID	Requirement	UCR 2013 Ref	LoC/ TP ID	R/O/C
IP6-6	**5.2.1.6 – Stateless Address Autoconfiguration and Manual Address Assignment**			
IP6-6-1	If the product supports stateless IP address autoconfiguration including those provided for the commercial market, then the product shall support IPv6 Stateless Address Autoconfiguration (SLAAC) for interfaces supporting UC functions in accordance with RFC 4862.	5.2.1.6 IP6-000420	L	C
IP6-6-2	If the product supports IPv6 SLAAC, then the product shall have a configurable parameter that allows the function to be enabled and disabled. Specifically, the product shall have a configurable parameter that allows the "managed address configuration" flag and the "other stateful configuration" flag to always be set and not perform stateless autoconfiguration.	5.2.1.6 IP6-000430	L	C
IP6-6-3	If the product supports IPv6 SLAAC, then the product shall have the configurable parameter set not to perform stateless autoconfiguration.	5.2.1.6 IP6-000440	L	C
IP6-6-4	While nodes are not required to auto configure their addresses using SLAAC, all IPv6 Nodes shall support link-local address configuration and Duplicate Address Detection (DAD) as specified in RFC 4862. In accordance with RFC 4862, DAD shall be implemented and shall be on by default. Exceptions to the use of DAD are noted in the following text.	5.2.1.6 IP6-000450	L	R
IP6-6-5	A node MUST allow for auto configuration related variable to be configured by system management for each multicast-capable interface to include Dup Addr Detect Transmits where a value of zero indicates that DAD is not performed on tentative addresses as specified in RFC 4862.	5.2.1.6 IP6-000460	L	R
IP6-6-6	The product shall support manual assignment of IPv6 addresses.	5.2.1.6 IP6-000470	L/T IO-2 IO-3	R
IP6-7	**5.2.1.7 – Internet Control Message Protocol**			
IP6-7-1	The product shall support the Internet Control Message Protocol (ICMP) for IPv6 as described in RFC 4443.	5.2.1.7 IP6-000520	L	R
IP6-7-2	The product shall support the capability to enable or disable the ability of the product to generate a Destination Unreachable message in response to a packet that cannot be delivered to its destination for reasons other than congestion.	5.2.1.7 IP6-000540	L	R
IP6-7-3	The product shall support the enabling or disabling of the ability to send an Echo Reply message in response to an Echo Request message sent to an IPv6 multicast or anycast address.	5.2.1.7 IP6-000550	L	R
IP6-7-4	The product shall validate ICMPv6 messages, using the information contained in the payload, before acting on them	5.2.1.7 IP6-000560	L	R
IP6-8	**5.2.1.8 – Routing Functions**			
IP6-8-1	The product shall support MLD as described in RFC 2710.	5.2.1.8 IP6-000680	L	R
IP6-9	**5.2.1.9 – IP Security**			
IP6-9-1	If the product uses IPSec, then the product shall be compatible with the Security Architecture for the IPSec described in RFC 4301. a. If RFC 4301 is supported, then the product shall support binding of a SA with a particular context. b. If RFC 4301 is supported, then the product shall be ca5pable of disabling the BYPASS IPSec processing choice.	5.2.1.9 IP6-000690	L	C
IP6-9-2	If RFC 4301 is supported, then the product shall not support the mixing of IPv4 and IPv6 in a SA.	5.2.1.9 IP6-000700	L	C
IP6-9-3	If RFC 4301 is supported, then the product's security association database (SAD) cache shall have a method to uniquely identify a SAD entry.	5.2.1.9 IP6-000710	L	C
IP6-9-4	If RFC 4301 is supported, then the product shall implement IPSec to operate with both integrity and confidentiality.	5.2.1.9 IP6-000720	L	C
IP6-9-5	If RFC 4301 is supported, then the product shall be capable of enabling and disabling the ability of the product to send an ICMP message informing the sender that an outbound packet was discarded.	5.2.1.9 IP6-000730	L	C
IP6-9-6	If an ICMP outbound packet message is allowed, then the product shall be capable of rate limiting the transmission of ICMP responses.	5.2.1.9 IP6-000740	L	C
IP6-9-7	If RFC 4301 is supported, then the system's Security Policy Database (SPD) shall have a nominal, final entry that discards anything unmatched.	5.2.1.9 IP6-000750	L	C

Table 3. IPv6 Requirements (continued)

ID	Requirement	UCR 2013 Ref	LoC/ TP ID	R/O/C
IP6-9-8	[Alarm] If RFC 4301 is supported, and the product receives a packet that does not match any SPD cache entries, and the product determines it should be discarded, then the product shall log the event and include the date/time, Security Parameter Index (SPI) if available, IPSec protocol if available, source and destination of the packet, and any other selector values of the packet.	5.2.1.9 IP6-000760	L	C
IP6-9-9	[Alarm] If RFC 4301 is supported, then the product should include a management control to allow an administrator to enable or disable the ability of the product to send an IKE notification of an INVALID_SELECTORS.	5.2.1.9 IP6-000770	L	C
IP6-9-10	If RFC 4301 is supported, then the product shall support the ESP Protocol in accordance with RFC 4303.	5.2.1.9 IP6-000780	L	C
IP6-9-11	RFC 4303 is supported, then the product shall be capable of enabling anti-replay.	5.2.1.9 IP6-000790	L	C
IP6-9-12	If RFC 4303 is supported, then the product shall check, as its first check, after a packet has been matched to its SA whether the packet contains a sequence number that does not duplicate the sequence number of any other packet received during the life of the security association.	5.2.1.9 IP6-000800	L	C
IP6-9-13	If RFC 4301 is supported, then the product shall support IKEv1 as defined in RFC 2409.	5.2.1.9 IP6-000810	L	C
IP6-9-14	To prevent a Denial of Services (DoS) attack on the initiator of an IKE_SA, the initiator shall accept multiple responses to its first message, treat each as potentially legitimate, respond to it, and then discard all the invalid half-open connections when it receives a valid cryptographically protected response to any one of its requests. Once a cryptographically valid response is received, all subsequent responses shall be ignored whether or not they are cryptographically valid.	5.2.1.9 IP6-000820	L	C
IP6-9-15	If RFC 4301 is supported, then the product shall support extensions to the Internet IP Security Domain of Interpretation for the Internet Security Association and Key Management Protocol (ISAKMP) as defined in RFC 2407.	5.2.1.9 IP6-000830	L	C
IP6-9-16	If RFC 4301 is supported, then the product shall support the ISAKMP as defined in RFC 2408.	5.2.1.9 IP6-000840	L	C
IP6-9-17	If the product supports the IPSec Authentication Header Mode, then the product shall support the IP Authentication Header (AH) as defined in RFC 4302.	5.2.1.9 IP6-000850	L	C
IP6-9-18	If RFC 4301 is supported, then the product shall support manual keying of IPSec.	5.2.1.9 IP6-000860	L	C
IP6-9-19	If RFC 4301 is supported, then the product shall support the ESP and AH cryptographic algorithm implementation requirements as defined RFC 4835	5.2.1.9 IP6-000870	L	C
IP6-9-20	If RFC 4301 is supported, then the product shall support the IKEv1 security algorithms as defined in RFC 4109.	5.2.1.9 IP6-000880	L	C
IP6-10	**5.2.1.10 – Network Management**			
IP6-10-1	If the product uses Uniform Resource Identifiers (URIs) in combination with IPv6, then the product shall use the URI syntax described in RFC 3986.	5.2.1.10 IP6-000990	L	C
IP6-11	**5.2.1.11 – Traffic Engineering**			
IP6-11-1	For traffic engineering purposes, the bandwidth required per voice subscriber is calculated to be 110.0 kbps (each direction) for each IPv6 call. This is based on G.711 (20 ms codec) with IP overhead (100 kbps) resulting in a 250-byte bearer packet plus 10 kbps for signaling, Ethernet Interframe Gap, and the Secure Real-Time Transport Control Protocol (SRTCP) overhead. Based on overhead bits included in the bandwidth calculations, vendor implementations may use different calculations and hence arrive at slightly different numbers.	5.2.1.11 IP6-001010	L	R
IP6-12	**5.2.1.12 – IP Version Negotiation**			
IP6-12-1	The product shall forward packets using the same IP version as the version in the received packet.	5.2.1.12 IP6-001040	L	R

Table 3. IPv6 Requirements (continued)

ID	Requirement	UCR 2013 Ref	LoC/ TP ID	R/O/C
IP6-13	**5.2.1.13 – Services Session Initiation Protocol IPv6 Unique Requirements**			
IP6-13-1	If the product is using AS-SIP, and the <addrtype>is IPv6, and the <connection-address> is a unicast address, then the product shall support generation and processing of unicast IPv6 addresses having the following formats: • x:x:x:x:x:x:x:x (where x is the hexadecimal values of the eight 16-bit pieces of the address). Example: 1080:0:0:0:8:800:200C:417A. • x:x:x:x:x:x:d.d.d.d (where x is the hexadecimal values of the six high-order 16-bit pieces of the address, and d is the decimal values of the four low-order 8-bit pieces of the address (standard IPv4 representation). For example, 1080:0:0:0:8:800:116.23.135.22.	5.2.1.13 IP6-001060	L	C
IP6-13-2	If the product is using AS-SIP, then the product shall support the generation and processing of IPv6 unicast addresses using compressed zeros consistent with one of the following formats: • x:x:x:x:x:x:x:x format: 1080:0:0:0:8:800:200C:417A. • x:x:x:x:x:x:d.d.d.d format: 1080:0:0:0:8:800:116.23.135.22. • Compressed zeros: 1080::8:800:200C:417A.	5.2.1.13 IP6-001070	L	C
IP6-13-3	If the product is using AS-SIP, and the <addrtype> is IPv6, and the <connection-address> is a multicast group address (i.e., the two most significant hexadecimal digits are FF), then the product shall support the generation and processing of multicast IPv6 addresses having the same formats as the unicast IPv6 addresses.	5.2.1.13 IP6-001080	L	C
IP6-13-4	If the product is using AS-SIP, and the <addrtype> is IPv6, then the product shall support the use of RFC 4566 for IPv6 in SDP as described in ASSIP 2013, Section 4, SIP Requirements for AS-SIP Signaling Appliances and AS-SIP EIs.	5.2.1.13 IP6-001090	L	C
IP6-13-5	If the product is using AS-SIP, and the <addrtype> is IPv6, and the <connection-address> is an IPv6 multicast group address, then the multicast connection address shall not have a Time To Live (TTL) value appended to the address as IPv6 multicast does not use TTL scoping.	5.2.1.13 IP6-001100	L	C
IP6-13-6	If the product is using AS-SIP, then the product shall support the processing of IPv6 multicast group addresses having the <number of address> field and may support generating the <number of address> field. This field has the identical format and operation as the IPv4 multicast group addresses.	5.2.1.13 IP6-001110	L	C
IP6-14	**5.2.1.14 – Miscellaneous**			
IP6-14-2	The products shall support Differentiated Services as described in RFC 2474 for a voice and video stream in accordance with Section 2, Session Control Products, and Section 6, Network Infrastructure End-to-End Performance, plain text DSCP plan.	5.2.1.14 IP6-001150	L	R
IP6-15	**Table 5.2-7 UC Information Assurance Security Devices**			
IP6-15-1	1981 Path MTU Discovery for IPv6	Table 5.2-7	L	R
	2407 The Internet IP Security Domain of Interpretation for ISAKMP	Table 5.2-7	L	C
	2408 Internet Security Association and Key Management Protocol (ISAKMP)	Table 5.2-7	L	C
	2409 The Internet Key Exchange (IKE)	Table 5.2-7	L	C
	2460 Internet Protocol, Version 6 (v6) Specification	Table 5.2-7	L	R-2
	2464 Transmission of IPv6 Packets over Ethernet Networks	Table 5.2-7	L	R-3
	2474 Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers	Table 5.2-7	L	R-4
	2710 Multicast Listener Discovery Version 2 (MLDv2) for IPv6	Table 5.2-7	L	R
	3162 RADIUS and IPv6	Table 5.2-7	L	C
	3986 Uniform Resource Identifier (URI): Generic Syntax	Table 5.2-7	L	C
	4007 IPv6 Scoped Address Architecture	Table 5.2-7	L	R
	4109 Algorithms for Internet Key Exchange Version 1 (IKEv1)	Table 5.2-7	L	C
	4213 Basic Transition Mechanisms for IPv6 Hosts and Routers	Table 5.2-7	L	R-1
	4291 IP Version 6 Addressing Architecture	Table 5.2-7	L	R
	4301 Security Architecture for the Internet Protocol	Table 5.2-7	L	C

Table 3. IPv6 Requirements (continued)

ID	Requirement		UCR 2013 Ref	LoC/ TP ID	R/O/C
IP6-15	**Table 5.2-7 UC Information Assurance Security Devices (continued)**				
	4302	IP Authentication Header	Table 5.2-7	L	C
	4303	IP Encapsulating Security Payload (ESP)	Table 5.2-7	L	C
	4443	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification	Table 5.2-7	L	R
	4566	SDP: Session Description Protocol	Table 5.2-7	L	C
	4835	Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)	Table 5.2-7	L	C
	4861	Neighbor Discovery for IP version 6 (IPv6)	Table 5.2-7	L	R
	4862	IPv6 Stateless Address Autoconfiguration	Table 5.2-7	L	C
	5095	Deprecation of Type 0 Routing Headers in IPv6	Table 5.2-7	L	R

LEGEND:

AES Advanced Encryption Standard
AS Assured Services
AS-SIP Assured Services Session Initiation Protocol
CAC Common Access Card
CRL Certificate Revocation List
DSCP Differentiated Services Code Point
EAP Extensible Authentication Protocol
FQDN Fully Qualified Domain Name
HMAC Hash-Based Message Authentication Code
IA Information Assurance
IAW In Accordance With
IDS Intrusion Detection System
IKE Internet Key Exchange
IP Internet Protocol
IPSec IP Security
IPv4 Internet Protocol version 4
IPv6 Internet Protocol version 6
MPLS Multiprotocol Label Switching
NIST National Institute of Standards and Technology
NMS Network Management System
NTP Network Transfer Protocol
NTPv3 Network Transfer Protocol version 3
OCSP Online Certificate Status Protocol
PKE Public Key Enable
PKI Public Key Infrastructure
RADIUS Remote Authentication Dial-in User Service
SBC Session Border Controller
SNMPv3 Simple Network Management Protocol version 3
SRTP Secure Real Time Protocol
SSH Secure Shell
SSL Secure Socket Layer
STIGs Security Technical Implementation Guideline
TLS Transport Layer Security
UCR Unified Capabilities Requirement
VVoIP Voice and Video over Internet Protocol

PRE TEST VALIDATION / STEPS

The test lab WAN routers, ASLAN components, telephony switches, RAE, and auxiliary equipment must be configured to integrate the SUT before the assessment begins. Verify the required network functionality is maintained as per the UCR 2013 Errata 1. Use Table 4, Test Checklist, to guide you before, during, and after testing.

Table 4. Test Checklist

Action No.	Requirements/Action (See note)	Completed Action Y/N/NA (Date)
Pre-Test Checklist (Before Testing)		
1	Prepare test documentation binder to include latest IO Test Plan and test status sheet. Test Procedures and test notes can be documented in a soft copy and saved on a shared drive. At JITC, Fort Huachuca, all documentation will be saved on T:\DISN TEST DELTA TEAM\VENDORS\. Note: test status sheet to be used during vendor weekly status meetings to brief status of test.	
2	Print the IO minutes from the T drive and put a copy in the test binder. See the lab manager if you cannot find a copy of the IO minutes.	
3	Download all SUT information from APLITS and save to the SUT folder on the share drive in a folder named 'APLITS data'. Review all of this data. Check APLITS for updates several times through the test.	
4	Ensure all required LoCs have been delivered by the vendor (download them from APLITS). Ensure they are based on the correct version of the UCR and are complete. Draft TDRs for all requirements not met or partially met based on the LoC(s).	
	Product LoC	
	IPv6 LoC	
	IA LoC	
	Draft TDRs based on LoCs (These must be reviewed and presented at the 1st status meeting.)	
	Other:	
5	If this is a DTR test, download everything from the DTR folder from APLITS and save it to the SUT folder on the T drive in a folder named "DTR#" (replace # with the DTR number).	
6	Ensure the SUT is integrated into the lab network, and that the network equipment is configured, including the UC WAN, ASLAN, RAE, and switches. Document this information.	
7	Receive Vendor POC email address, Mailing address, and telephone number (business cards)	
8	Coordinate with vendor to lock down system login/passwords. After login passwords are reconfigured by tester ensure they are saved in the SA password database.	
9	Obtain latest version of IO Cert template to use for the SUT.	
10	Identify SUT product type per UCR 2013 Errata 1. Verify with vendor the exact nomenclature of SUT and insert in subject line, Memo header, and Summary title, and SUT tables of IO cert template: Example: Cisco Aggregation Services Router (ASR) 9000 with Internetwork Operating System (IOS) XR 4.3.2	
11	Verify SUT test diagram with vendor and visibly verify all components, subcomponents, and interfaces.	
12	Document and capture soft copy of SUT configurations (Hardware/Software). Obtain screen captures for each piece of equipment. Do not use the IA captures. Fill in Joint IO cert tables (Memo Table 4, Enclosure 3 Table 3-3).	
13	Review all components and subcomponents the vendor submitted to APLITS, which they want JITC to analyze as similar for interoperability purposes. After review fill in IO cert tables (Memo Table 4, Enclosure 3 Table 3-3). Bold and underline tested components/ subcomponents. As applicable copy previous version of table and redline new systems/versions.	
14	If this test effort is a V&V ensure that all of the SUT subcomponent versions are certified versions with the exception of the software changes associated with the V&V.	
15	Verify all interfaces on SUT to be tested and fill in IO Cert Memo Table 2.	
16	Document all components in the test architecture in the IO Cert Memo Table 3-4. Include all LSCs, SSs, legacy switches, SBCs, network IP switches, telephones, DSCDs, special test equipment, etc.	
17	Refer to APLITs for system description. Fill in description in IO cert Enclosure 2, paragraph 5. Remove all vendor marketing language and IA fluff. Compare with IA to ensure they are congruent.	

Table 4. Test Checklist (continued)

Action No.	Requirements/Action	Completed Action Y/N/NA (Date)
18	Identify any open TDRs that have been adjudicated with Vendor PoAMs to ensure that stipulated PoAM dates have not expired without a fix. If a TDR was adjudicated as Minor with PoAM and the PoAM date has expired you will need to submit the TDR to the AO requesting a new PoAM from the vendor. Once the PoAM is received the TDR is submitted to DISA for adjudication.	
In-Test Checklist		
1	Put away test documents (Test Plan, Capture Logs, etc) at end of test day	
2	Do not discuss or air vendor "dirty laundry" in front of other vendors	
3	Do not pass on frivolous information to the Government. Know what the issues are if you are not sure or have not put a thumb on a problem don't disclose it until you do.	
4	Ensure and control security of login/password control during testing.	
5	Keep your test areas of responsibilities clean	
6	Think outside the box	
7	Once TDRs are reviewed, they will be discussed in the weekly status meetings. PoAMs are due from the vendor within five business days.	
8	Verify that all required test items per the TP have been tested and are met.	
9	Verify that all required items are met by testing and/or LOC.	
10	Review with the vendor untested condition or optional requirements to verify if they are supported/not tested or not supported.	
11	Annotate Redlines to the TP as appropriate.	
12	Update TDRs with the vendor PoAMs. Save the updated TDRs to the shared drive and provide the electronic copy to the lab manager.	
13	Schedule the final out-brief to occur within five business days of the end of testing.	
Post-Testing Checklist		
1	Prepare and submit the draft Joint Interoperability Certification to the Lab Manager and Technical Editor for review within one week after testing is completed.	
2	If this is a DTR test at JITC, Fort Huachuca, the technical editor (Sarah) will draft the extension based on tester input. Provide all relevant data, including the actual test dates, hardware/software changes, closed TDRs, new TDRs, PoAM review, etc. If the hardware/software changed, use the previous SUT table and not changes to it.	
3	Ensure that testing log and other pertinent documents are filed appropriately.	
4	Be prepared to answer questions about the system, TDRs, and testing.	

NOTES:
See Pre-Test Checklist Companion Guide for More details.

LEGEND:

AO	Action Officer	LOC	Letter of Conformance
APLITS	Approved Products List Integrated Tracking System	PoAM	Plan of Action and Milestones
ASLAN	Assured Service Local Area Network	RAE	Required Ancillary Equipment
DISA	Defense Information Systems Agency	SUT	System Under Test
DTR	Desktop Review	TDR	Test Discrepancy Report
GAO	Government Action Officer	TN	Tracking Number
IA	Information Issuance	TP	Test Plan
IO	Interoperability	UC	Unified Capabilities
IPv6	Internet Protocol version 6	UCCO	Unified Capabilities Connection Office
JITC	Joint Interoperability Test Command	WAN	Wide Area Network

TEST PROCEDURES

Test Procedure No: IO-1
Requirement ID: SCM-008620 SCM-008630, SCM-008640
Name: Differentiated Services Code Point Packet Marking
Reference: UCR 2013 Sections: 2.17.4
Applicability: SBC (Optional)

Objective:

The SBC shall ensure that media streams associated with a particular session use the appropriate DSCP based on the information in the AS-SIP RPH (OPTIONAL). Packets that are not marked with the appropriate DSCP shall be dropped (OPTIONAL). The SBC shall perform this policing for media packets received from the ASLAN that are destined for points outside of the ASLAN, and for media packets received from the WAN that are destined for points within the ASLAN (OPTIONAL). Table 5 depicts the appropriate DSCP markings

Table 5. DSCP Marking Requirements

AGGREGATED SERVICE CLASS	GRANULAR SERVICE CLASS	PRIORITY/ PRECEDENCE	DSCP DECIMAL	DSCP IPv4 HEX	DSCP IPv6 HEX
Network Control	Network Signaling (OSPF, BGP, etc)	N/A	48	0x30	0xC0
Inelastic Real-Time	User Signaling (AS-SIP, H.323, etc.)	N/A	40	0x28	0xA0
	Short Message	FO	32	0x20	0x80
	Assured Voice (Includes SRTCP)	FO	41	0x29	0XA4
		F	43	0x2B	0xAC
		I	45	0x2D	0XB4
		P	47	0x2F	0xBC
		R	49	0x31	0XC4
	Non-Assured Voice*	N/A	46	0x2E	0Xb8
	Assured Multimedia Conferencing (voice, video, data)	FO	33	0x21	0x84
		F	35	0x23	0x8C
		I	37	0x25	0x94
		P	39	0x27	0x9C
		R	51	0x33	0xCC
	Broadcast Video	N/A	24	0x18	0x60

Table 5. DSCP Marking Requirements (continued)

AGGREGATED SERVICE CLASS	GRANULAR SERVICE CLASS	PRIORITY/ PRECEDENCE	DSCP DECIMAL	DSCP IPv4 HEX	DSCP IPv6 HEX
Inelastic Real-Time	Non-Assured Multimedia Conferencing (34, 36, and 38)	VOICE	34**	0x22	0x88
		VIDEO	36**	0x24	0x90
		DATA	38**	0x26	0x98
Preferred Elastic	Multimedia Streaming	FO	24	0x18	0x60
		F	25	0x19	0x64
		I	27	0x1B	0x6C
		P	31	0x1F	0x7C
		R	26 (28, 30)**	0x1A	0x68
	Low-Latency Data: (IM, Chat, Presence)	FO	17	0x11	0x44
		F	19	0x13	0x4C
		I	29	0x1D	0x74
		P	23	0x17	0x5C
		R	18 (20, 22)**	0x12	0x48
	High Throughput Data	FO	9	0x9	0x24
		F	11	0xB	0x2C
		I	13	0xD	0x34
		P	15	0xF	0x3C
		R	10 (12, 14)**	0xA	0x28
	OA&M	N/A	16	0x10	0x40
Elastic	Best Effort	N/A	0	0x0	0x0
	Low Priority Data	N/A	8	0x8	0x20

LEGEND:

AS-SIP	Assured Services Session Initiation Protocol
BGP	Border Gateway Protocol
DSCP	Differentiated Services Code Point
F	FLASH
FO	FLASH OVERRIDE
I	IMMEDIATE
IM	Instant Messaging
N/A	Not Applicable
OA&M	Operations, Administration, and Maintenance
OSPF	Open Shortest Path First
P	PRIORITY
R	ROUTINE
SRTCP	Secure Real-Time Transport Control Protocol

Test Setup:

1. Configure the end instrument or its servicing LSC to send the incorrect DSCP value for each precedence of call made.
2. Configure Wireshark on a PC connected to a tap hooked to the red side of the SBC to monitor traffic in and out of the SBC. At JITC, perform the capture by using a lab network PC loaded with Wireshark to connect to the appropriate MEDIA capture server.
3. For non-VoIP End Instruments, set up Wireshark on a VoIP EI and capture calls coming into that EI from the non-VoIP EI in order to verify the SBC's behavior.
4. Perform test procedures with the SUT as the ON and then repeat with the SUT as the DN.- TURN ON WIRESHARK CAPTURE PRIOR TO BEGINNING THE TEST PROCEDURE.

Test Procedures:

1. Place a ROUTINE call with the incorrect DSCP value from ON1 to DN1 through the SBC. Hang up call.
2. Stop Wireshark.
3. Open the Wireshark capture and attempt to locate UDP packets for the call.
4. Verify that the UDP packets with the incorrect values were dropped by the SBC (OPTIONAL).
5. If the media packets weren't dropped, find the Internet Protocol (IP) header in the UDP packet. Expand the IP header until you find the Differentiated Services Field. Verify that the media packets are marked with the DSCP sent by the end instrument/LSC. Refer to Table 5 for the correct values by stream type and precedence.
6. Repeat for all precedence levels (Priority, Immediate, Flash, and Flash-Override)
7. Repeat the procedure with the end instrument or LSC sending no DSCP in the media streams.
8. Repeat procedures for every applicable phone type on the SUT.
9. Repeat procedures with the SUT as the DN.

Data Required: Refer to Excel data collection form.

Test Procedure No: IO-2
Requirement ID(s): SCM-000250
Name: Call Hold
Reference: UCR 2013 Sections: 2.5
Applicability: SBC

Objective: SBCs must process calls on hold.

Test Setup:
1. All EIs used as DN1 for this test procedure can have a single or multiple appearances.
2. Perform test procedures with the SUT as the ON and then repeat with the SUT as the DN.
3. START PACKET CAPTURE PRIOR TO BEGINNING THE TEST PROCEDURE.
4. All test procedures will be done bi-directionally.

Test Procedures:
Inter-Switch:
Invocation of Call Hold
1. Place a ROUTINE call from ON1 to DN1.
    a. ON1 to DN1 call completes.
    b. DN1 places ON1 on hold by going “on-hook” then “off-hook”.
    c. ON1 receives MoH, if supported by the SC.
    d. DN1 retrieves ON1 from hold.
    e. Verify ON1 and DN1 remain connected at ROUTINE, with two-way speech path.
2. Repeat using all available phone types on the SC for DN1.
3. Repeat with the SUT as DN.

Call Hold Preempt Holdee
1. Place a ROUTINE call from ON1 to DN1.
    a. ON1 to DN1 call completes.
    b. ON1 places DN1 on hold, and calls DN2.
    c. DN1 receives MoH, if supported by the SC.
    d. ON1 to DN2 call completes.
    e. Place a PRIORITY call from ON2 to DN1.
    f. DN1 receives PNT and goes on hook.
    g. ON1 and DN2 remain connected with no PNT.
    h. ON1 attempts to retrieve DN1 from call hold state.
    i. ON1 receives PNT. (*ON1 will only receive PNT if it attempts to retrieve DN1 call while PNT is being played at DN1).
    j. After DN1 goes on hook.
    k. DN1 rings at precedence cadence.
    l. DN1 goes off hook to connect with ON2.
2. Place all phones on hook
3. Repeat with the SUT as DN.

Call Hold Preempt Holder
1. Place a ROUTINE call from ON1 to DN1.
    a. ON1 to DN1 call completes
    b. ON1 places DN1 on hold, and calls DN2.
    c. DN1 receives MoH, if supported by SC.
    d. ON1 to DN2 call completes.

e. Place a PRIORITY call from ON2 to ON1.
f. ON1, DN1 and DN2 receive PNT and go on hook.
g. ON1 Rings at Precedence above ROUTINE cadence.
h. ON2 to ON2 call completes.

2. Place all phones on hook
3. Repeat with the SUT as DN.

Call Hold Preempt Active

1. Place a ROUTINE call from ON1 to DN1.
   a. ON1 to DN1 call completes.
   b. ON1 places DN1 on hold, and calls DN2.
   c. DN1 receives MoH, if supported by SC.
   d. ON1 to DN2 call completes.
   e. Place a PRIORITY call from ON2 to DN2.
   f. ON1 and DN2 receive PNT and go on hook.
   g. DN2 rings at precedence above ROUTINE cadence.
   h. ON2 to DN2 call completes.
   i. After placing ON1 on hook.
   j. ON1 rings at ROUTINE cadence.
   k. ON1 goes off hook and reconnects with DN1.
2. Place all phones on hook
3. Repeat with the SUT as DN.

Data Required: Refer to Excel data collection form.

Test Procedure No: IO-2a
Requirement ID(s): SCM-000020, SCM-000030, SCM-000040, SCM-000050
Name: Call Forwarding Variable
Reference: UCR 2013, Section 2.2, 2.2.1 AND 2.2.1.1; and Table 2.2-1
Applicability: SBC

Objective: SBC must support Call Forwarding.

Test Setup:
1. All EIs used as ON1 and DN1 for this test procedure can have a single or multiple appearances.
2. Perform test procedures with the SUT as the ON and then repeat with the SUT as the DN.
3. Turn on packet capture prior to beginning of each test procedure.

Test Procedures:

Call Forwarding Variable, Calling Inter-environment **(With MLPP Interaction)**:
1. Activate CFV on DN1 forwarding to DN2.
2. Start a call capture at the SUT and/or another SBC.
3. Place a ROUTINE call from ON1 to DN1.
   a. DN1 forwards the call to DN2 and gives CFV “ping ring” notification.
   b. DN1 to DN2 call completes.
   c. Place all phones on hook.
4. Place a PRIORITY call from ON1 to DN1.
   a. DN1 forwards the call to DN2 and gives CFV “ping ring” notification.
   b. ON1 to DN2 call completes.
   c. Place all phones on hook.
5. Place an IMMEDIATE call from ON1 to DN1.
   a. DN1 forwards the call to DN2 and gives CFV “ping ring” notification.
   b. ON1 to DN2 call completes.
   c. Place all phones on hook.
6. Place a FLASH call from ON1 to DN1.
   a. DN1 forwards the call to DN2 and gives CFV “ping ring” notification.
   b. ON1 to DN2 call completes.
   c. Place all phones on hook.
7. Place a FLASH OVERRIDE call from ON1 to DN1.
   a. DN1 forwards the call to DN2 and gives CFV “ping ring” notification.
   b. ON1 to DN2 call completes.
   c. Place all phones on hook.
8. Replace DN1 with DN4 (Soft Phone) and repeat 1 thru 7.
9. Repeat test steps with the SUT as the DN.

1. Call Forwarding Variable, Call Forwarded Inter-environment (With MLPP Interaction)
2. Activate CFV on DN1 forwarding to ON1.
3. Start a call capture at the SUT and/or another SBC.
4. Place a ROUTINE call from ON2 to DN1.
   a. Verify DN1 forwards to ON1, and gives “ping ring” notification.
   b. ON2 to ON1 call completes.
   c. Place all phones on hook.

5. Place a PRIORITY call from ON2 to DN1.
    a. Verify DN1 forwards to ON1, and gives “ping ring” notification.
    b. ON2 to ON1 call completes.
    c. Place all phones on hook.
6. Place an IMMEDIATE call from ON2 to DN1.
    a. Verify DN1 forwards to ON1, and gives “ping ring” notification.
    b. ON2 to ON1 call completes.
    c. Place all phones on hook.
7. Place a FLASH call from ON2 to DN1.
    a. Verify DN1 forwards to ON1, and gives “ping ring” notification.
    b. ON2 to ON1 call completes.
    c. Place all phones on hook.
8. Place a FLASH OVERRIDE call from ON2 to DN1.
    a. Verify DN1 forwards to ON1, and gives “ping ring” notification.
    b. ON2 to ON1 call completes.
    c. Place all phones on hook.
9. Replace DN1 with DN4 (Soft Phone) and repeat 1 thru 8.
10. Repeat test steps 1-9 with the SUT as the DN.

Remove CFV from all phones prior to beginning the next test procedure.

Call Forwarding Variable, Call Forwarded Inter-environment (**Without MLPP Interaction)**:

1. Activate CFV on DN1 forwarding to ON1.
    a. Place a ROUTINE call from DN2 to DN1.
    b. Verify DN1 forwards to ON1, and gives “ping ring” notification.
    c. DN2 to ON1 call completes.
    d. Place all phones on hook.
2. Place a PRIORITY call from DN2 to DN1.
    a. Verify CFV is not activated, and the call is instead diverted to the designated destination.
    b. Place all phones on hook.
3. Place an IMMEDIATE call from DN2 to DN1.
    a. Verify CFV is not activated, and the call is instead diverted to the designated destination.
    b. Place all phones on hook.
4. Place a FLASH call from DN2 to DN1.
    a. Verify CFV is not activated, and the call is instead diverted to the designated destination.
    b. Place all phones on hook.
5. Place a FLASH OVERRIDE call from DN2 to DN1.
    a. Verify CFV is not activated, and the call is instead diverted to the designated destination.
    b. Place all phones on hook.
6. Repeat test steps 1-5 with the SUT as the DN.

Remove CFV from all phones prior to beginning the next test procedure.

Data Required: Refer to Excel data collection form.

Test Procedure No: IO-2b
Requirement ID(s): SCM-000060, SCM-000070, SCM-000130
Name: Call Forwarding Busy Line
Reference: UCR 2013, Section 2.2.1.2 and 2.2.2.1
Applicability: SBC

Objective: SBC must support Call Forwarding.

Test Setup:
1. All EIs used as DN1 for this test procedure can have a single or have multiple appearances with one appearance busy with a FLASH OVERRIDE call.
2. Perform test procedures with the SUT as the ON and then repeat with the SUT as the DN.
3. Turn on packet capture prior to beginning of each test procedure.

Test Procedures:

Call Forwarding Busy Line, Calling Inter-environment:
1. Activate CFB on DN1 forwarding to DN2.
2. Place a ROUTINE call from ON1 to DN1.
   a. DN1 forwards the call to DN2.
   b. Place all phones on hook.
   c. Place a PRIORITY call from ON1 to DN1.
   d. DN1 forwards call to DN2.
   e. Place all phones on hook.
3. Place an IMMEDIATE call from ON1 to DN1.
   a. ON1 is forwarded to DN2.
   b. Place all phones on hook.
4. Place a FLASH call from ON1 to DN1.
   a. ON1 is forwarded to DN2.
   b. Place all phones on hook.
5. Place a FLASH OVERRIDE call from ON1 to DN1.
   a. ON1 is forwarded to DN2
   b. Place all phones on hook.
6. Repeat test steps with the SUT as the DN.

Call Forward Busy: Higher incoming precedence.
1. Activate CFB from ON1 forwarding to DN3
2. Place a ROUTINE call from ON1 to DN4.
   a. Call completes
   b. Place a PRIORITY call from DN2 to ON1
   c. ON1 and DN4 receive PNT and go on hook
   d. DN2 completes to ON1.
3. Place an IMMEDIATE call from DN4 to ON1
   a. ON1 and DN2 receive PNT and go on hook
   b. DN4 completes to ON1
4. Place a FLASH call from DN2 to ON1.
   a. ON1 and DN4 receive PNT and go on hook
   b. DN2 completes to ON1.
5. Place a FLASH OVERRIDE call from DN4 to ON1.
   a. ON1 and DN2 receive PNT and go on hook

   b. DN4 completes to ON1
6. Place all instruments on hook.
7. Repeat test steps with the SUT as the DN.

Call Forward Busy: Equal or lower precedence.

1. Activate CFB from ON1 forward to ON3
2. Place a ROUTINE call from ON1 to DN2.
   a. Call completes
   b. Place a ROUTINE call from DN4 to ON1
   c. DN4 forwards to ON3
   d. Place all instruments on hook
3. Place a PRIORITY call from ON1 to ON2. Call completes
   a. Place a ROUTINE call from DN4 to ON1.
   b. DN4 forwards to ON3.
   c. Place all instruments on hook.
4. Place a PRIORITY call from ON1 to DN2.
   a. Place a PRIORITY call from DN4 to ON1.
   b. DN4 forwards to ON3
   c. Place all instruments on hook.
5. Repeat test steps with the SUT as the DN.

Call Forward Busy: Non-preemptable

1. Activate CFB from ON3 (non-preemptable) forward to DN2
2. Place a ROUTINE call from ON1 to ON3
   a. Call completes.
   b. Place a PRIORITY call from DN4 to ON3
   c. DN4 forwards to DN2
   d. Place all instruments on hook
3. Place a ROUTINE call from DN1 to ON3.
   a. Call Completes
   b. Place a ROUTINE call from ON4 to ON3
   c. ON4 forwards to DN2
   d. Place all instruments on hook.
4. Place a PRORITY call from ON1 to ON3.
   a. Call Completes
   b. Place a PRIORITY call from DN4 to ON3
   c. DN4 forwards to DN2
   d. Place all instruments on hook.
5. Place a PRORITY call from DN1 to ON3.
   a. Call Completes
   b. Place a ROUTINE call from ON4 to ON3
   c. ON4 forwards to DN2
   d. Place all instruments on hook
6. Repeat test steps with the SUT as the DN.

Call Forward Busy: Precedence Level Preserved 1.

1.Activate CFB from ON1 forward to ON3.
2.Place a PRIORITY call from DN2 to ON1. Call completes.
3.Place a ROUTINE call from DN4 to ON3. Call Completes.

4.Place a PRIORITY call from DN5 to ON1.
   a. DN5 forwards to ON3, preempting DN4 and ON3.
   b. DN4 and ON3 receive PNT and go on hook.
   c. DN5 and ON3 complete.
   d. DN2 and ON1 remain in a call.
   e. Place all instruments on hook.
5. Repeat test steps with the SUT as the DN.

Call Forward Busy: Forwarded to DN is Unanswered

1. Setup alternate DN or Attendant on the switches supporting the ON and DN end instruments.
2. Activate CFB from ON1 forward to ON3.
3. Place a PRIORITY call from DN2 to ON1.
   a. Call completes.
   b. Place a PRIORITY call from DN5 to ON1.
   c. Call forwards to ON3. Allow ON3 to ring unanswered.
   d. DN5 diverts to an alternate DN or Attendant.
   e. Place all instruments on hook.

4.Repeat test steps with the SUT as the DN.

Data Required: Refer to Excel data collection form.

Test Procedure No: IO-2c
Requirement ID(s): SCM-000080, SCM-000090, SCM-000140, SCM-000150
Name: Call Forwarding - Do Not Answer – All Calls
Reference: UCR 2013, Section 2.2.1.3 and 2.2.2.2
Applicability: SBC

Objective: SBC must support Call Forwarding.

Test Setup:
1. All EIs used as ON1 for this test procedure can have a single or multiple appearances with one appearance busy with a FLASHOVERRIDE call.
2. Perform test procedures with the SUT as the ON and then repeat with the SUT as the DN.
3. Turn on packet capture prior to beginning of each test procedure.

Test Procedures:

If MLPP is supported complete the following tests:

Call Forward No Answer Precedence is Preserved
1. Setup up Call Forward No Answer on ON1 forwarding to ON3
2. Place a ROUTINE call from DN2 to ON3.
   a. Call completes
   b. Place a PRIORITY call from DN4 to ON1
   c. DN2 and ON3 receive PNT and go on hook
   d. DN4 and ON3 complete
   e. Place all instruments on hook.
3. Place a PRIORITY call from DN2 to ON3
   a. Call completes
   b. Place a IMMEDIATE call from DN4 to ON1
   c. DN2 and ON3 receive PNT and go on hook
   d. ON4 and ON3 complete
   e. Place all instruments on hook.
4. Place a IMMEDIATE call from DN2 to ON3
   a. Call completes
   b. Place a FLASH call from DN4 to ON1
   c. DN2 and ON3 receive PNT and go on hook
   d. DN4 and ON3 complete
   e. Place all instruments on hook.
   f. Place a FLASH call from DN2 to ON3
   g. Call completes
5. Place a FLASHOVERRIDE call from DN4 to ON1
   a. DN2 and ON3 receive PNT and go on hook
   b. DN4 and ON3 complete
   c. Place all instruments on hook.
   d. Repeat test steps with the SUT as the DN.

Forward No Answer, DN busy with Equal Precedence

1. Place a PRIORITY call from DN2 to ON3
   a. Call completes.
   b. Place a PRIORITY call from DN4 to ON1 ring no answer
   c. DN4 forwards to ON3
   d. DN4 receive a Block Precedence Announcement (BPA) or diverts to the attendant.
2. Repeat test steps with the SUT as the DN.

Forward No Answer, DN Unanswered to Alternate DN or Attendant

1. Setup alternate DN or Attendant on the switches supporting the ON and DN end instruments.
2. Place a PRIORITY call from DN2 toON1 ring no answer
   a. DN2 forward to ON3 ring no answer.
   b. DN2 forwards to an alternate DN or attendant.
3. Repeat test steps with the SUT as the DN.

Data Required: Refer to Excel data collection form.

Test Procedure No: IO-2d
Requirement ID(s): SCM-000160, SCM000170, SCM-000180, SCM-000200, SCM-000210
Name: Precedence Call Waiting
Reference: UCR 2013 Sections: 2.2.3, 2.2.3.1, 2.2.3.2, 2.2.3.4, 2.2.3.5 and 2.2.3.6
Applicability: SBC

Objective: SBCs must process IP-to-IP call waiting.

Test Setup:
1. All EI's used as DN2 for this test procedure must have either have a single appearance or dual appearance with one appearance busy with a Flash Override call.
2. Perform test procedures with the SUT as the ON and then repeat with the SUT as the DN.
3. -TURN ON PACKET CAPTURE BEFORE STARTING THE TEST PROCEDURE.

Test Procedures:

Busy with higher precedence:
1. Place an IMMEDIATE call from ON1 to DN2.
   a. Verify call completes.
   b. Place a PRIORITY call from ON3 to DN2.
   c. Verify DN2 receives precedence call waiting tone.
   d. DN2 accepts waiting call.
   e. ON3 to DN2 call completes.
   f. DN2 switches back to ON1 call.
   g. Verify DN2 is able to retrieve ON1.
   h. Place all instruments on hook.
2. Repeat test steps with the SUT as the DN.

Busy with equal precedence:
1. Place a PRIORITY call from ON1 to DN2.
   a. Verify call completes.
   b. Place a PRIORITY call from ON3 to DN2.
   c. Verify DN2 receives precedence call waiting tone.
   d. DN2 accepts waiting call.
   e. ON3 to DN2 call completes.
   f. DN2 switches back to ON1 call.
   g. **Verify DN2 is able to retrieve ON1.**
   h. Place all instruments on hook.
2. Repeat test steps with the SUT as the DN.

Busy with lower precedence:
1. Place a ROUTINE call from ON1 to DN2.
   a. Verify call completes.
   b. Place a PRIORITY call from ON3 to DN2.
   c. Verify ON1 and dN2 receive PNT.
   d. ON3 to DN2 call completes.
   e. Place an IMMEDIATE call from ON1 to DN2.
   f. Verify DN2 and ON3 receive PNT.
   g. ON1 to DN2 call completes.
   h. Place a FLASH call from ON3 to DN2.

i. Verify DN2 and ON1 receive PNT.
j. ON3 to DN2 call completes.
k. Place a FLASH OVERRIDE call from ON1 to DN2.
l. Verify DN2 and ON3 receive PNT.
m. ON1 to DN2 call completes.
n. Place all instruments on hook

2. Repeat test steps with the SUT as the DN.

No answer:

1. Setup alternate DN or Attendant on the switches supporting the ON and DN end instruments.
2. Place an IMMEDIATE call from ON1 to DN2.
   a. Verify call completes.
   b. Place a PRIORITY call from ON3 to DN2.
   c. Verify DN2 receives precedence call waiting tone.
   d. Do not answer ON3 call.
   e. ON3 call diverts to attendant console or alternate DN within 15 to 45 seconds.
   f. Place all instruments on hook.
3. Repeat test steps with the SUT as the DN.

Verify Precedence is maintained for subsequent calls:

1. Place a FLASH call from ON1 to DN2.
   a. Verify call completes.
   b. Place a PRIORITY call from ON3 to DN2.
   c. Verify DN2 receives precedence call waiting tone.
   d. DN2 accepts waiting ON3 call.
   e. ON3 to DN2 call completes.
   f. DN2 switches back to ON1 call.
   g. Place ON3 on hook.
   h. Verify DN2 is able to retrieve ON1.
   i. Place an IMMEDIATE call from ON3 to DN2.
   j. Verify DN2 receives precedence call waiting tone.
   k. DN2 accepts waiting ON3 call.
   l. ON3 to DN2 call completes.
   m. Place all instruments on hook.
2. Repeat test steps with the SUT as the DN.

Data Required: Refer to Excel data collection form.

Test Procedure No: IO-2e
Requirement ID(s): SCM-000220, SCM-000230, SCM-000240
Name: Call Transfer
Reference: UCR 2013 Sections: 2.2.4, 2.2.4.1 and 2.2.4.2
Applicability: SBC

Objective: SBCs must process call transfers.

Test Setup:
1. All EIs used as transferor for this test procedure may have a dual appearance.
2. The ASAC budget between the SC and the transferor should at least 2.
3. Perform the procedure where the transferor uses the **REFER** method.
4. Repeat the procedure where the transferor uses the **INVITE/RE-INVITE** method.
5. Perform test procedures with the SUT as the ON and then repeat with the SUT as the DN.
6. TURN ON PACKET CAPTURE/PRIOR TO BEGINNING THE TEST PROCEDURE.

Calling Inter-Environment:
Normal Call Transfer (Attended):
1. Place a PRIORITY call from ON1 to DN1.
    a. ON1 to DN1 call completes.
    b. DN1 normal call transfers ON1 to DN2.
    c. ON1 to DN2 call completes at PRIORITY.
    d. Place DN1 on hook.
    e. ON1 to DN2 remain connected.
    f. Place a ROUTINE call from ON2 to DN2.
    g. ON2 receives standard busy tone, or is connected to voicemail.
    h. Place ON2 on hook.
    i. Place a PRIORITY call from ON2 to ON1.
    j. ON2 receives BPA or diverts appropriately.
    k. Place ON2 on hook.
    l. Place an IMMEDIATE call from ON2 to DN2.
    m. ON1 and DN2 receive PNT and go on hook
    n. ON2 to DN2 call completes.
    o. Place all instruments on hook.
2. Repeat test steps with the SUT as the DN.

Normal Call Transfer (Unattended):

1. Place a PRIORITY call from ON1 to DN1.
   a. ON1 to DN1 call completes.
   b. DN1 normal call transfers ON1 to DN2; do not answer DN2.
      DN1 hangs up before DN2 answers; answer DN2.
   c. ON1 to DN2 call completes.
   d. Place a ROUTINE call from ON2 to DN2.
   e. ON2 receives a standard busy tone, or is connected to voicemail.
   f. Place ON2 on hook.
   g. Place a PRIORITY call from ON2 to ON1.
   h. ON2 receives BPA or diverts appropriately.
   i. Place ON2 on hook.
   j. Place an IMMEDIATE call from ON2 to DN2.
   k. ON1 and DN2 receive PNT and go on hook.
   l. ON2 to DN2 call completes.
   m. Place all instruments on hook.
2. Repeat test steps with the SUT as the DN.

Explicit Call Transfer (Attended):

1. Place a PRIORITY call from ON1 to DN1.
   b. ON1 to DN1 call completes.
   c. ON1 transfers DN1 to ON2.
   d. DN1 to ON2 call completes at PRIORITY.
   e. Place a ROUTINE call from ON1 to DN1.
   f. ON1 receives standard busy tone or is connected to voicemail.
   g. Place ON1 on hook.
   h. Place a PRIORITY call from ON1 to ON2.
   i. ON1 receives a BPA or diverts appropriately.
   j. Place ON1 on hook.
   k. Place an IMMEDIATE call from ON1 to DN1.
   l. DN1 and ON2 receive PNT and go on hook.
   m. ON1 to DN1 call completes.
   n. Place all instruments on hook.
2. Repeat test steps with the SUT as the DN.

Explicit Call Transfer (Unattended):

1. Place a PRIORITY call from ON1 to DN1.
   a. ON1 to DN1 call completes.
   b. ON1 transfers DN1 to ON2; don't answer.
   c. ON1 hangs up before ON2 answers; answer ON2.
   d. DN1 to ON2 call completes at PRIORITY.
   e. Place a ROUTINE call from ON1 to DN1.
   f. ON1 receives a standard busy tone.
   g. Place ON1 on hook.
   h. Place a PRIORITY call from ON1 to ON2.
   i. ON1 receives BPA or diverts appropriately.
   j. Place ON1 on hook.
   k. Place an IMMEDIATE call from ON1 to DN1.
   l. DN1 and ON2 receive PNT and go on hook.
   m. ON1 to DN1 call completes.

n. Place all instruments on hook.
2. Repeat test steps with the SUT as the DN.

Call Transferred Inter-Environment:
Normal Call Transfer (Attended):
1. Place a PRIORITY call from ON1 to ON2.
   a. ON1 to ON2 call completes.
   b. ON2 normal call transfers ON1 to DN1.
   c. ON1 to DN1 call completes at PRIORITY.
   d. Place ON2 on hook.
   e. ON1 to DN1 remain connected.
   f. Place a ROUTINE call from ON2 to DN1.
   g. ON2 receives standard busy tone, or is connected to voicemail.
   h. Place ON2 on hook.
   i. Place a PRIORITY call from ON2 to ON1.
   j. ON2 receives BPA or diverts appropriately.
   k. Place ON2 on hook.
   l. Place an IMMEDIATE call from ON2 to DN1.
   m. ON1 and DN1 receive PNT and go on hook.
   n. ON2 to DN1 call completes.
   o. Place all instruments on hook.
2. Repeat test steps with the SUT as the DN.

Normal Call Transfer (Unattended):
1. Place a PRIORITY call from ON1 to ON2.
   a. ON1 to ON2 call completes.
   b. ON2 normal call transfers ON1 to DN1; do not answer DN1.
   c. ON2 hangs up before DN1 answers; answer DN1.
   d. ON1 to DN1 call completes.
   e. Place a ROUTINE call from ON2 to DN1.
   f. ON2 receives a standard busy tone, or is connected to voicemail.
   g. Place ON2 on hook.
   h. Place a PRIORITY call from ON2 to ON1.
   i. ON2 receives BPA or diverts appropriately.
   j. Place ON2 on hook.
   k. Place an IMMEDIATE call from ON2 to DN1.
   l. ON1 and DN1 receive PNT and go on hook.
   m. ON2 to DN1 call completes.
   n. Place all instruments on hook.
2. Repeat test steps with the SUT as the DN.

Explicit Call Transfer (Attended):
1. Place a PRIORITY call from ON1 to ON2.
   a. ON1 to ON2 call completes.
   b. ON1 transfers ON2 to DN1.
   c. ON2 to DN1 call completes at PRIORITY.
   d. Place a ROUTINE call from ON1 to DN1.
   e. ON1 receives standard busy tone or is connected to voicemail.
   f. Place ON1 on hook.

g. Place a PRIORITY call from ON1 to ON2.
h. ON1 receives a BPA or diverts appropriately.
i. Place ON1 on hook.
j. Place an IMMEDIATE call from ON1 to DN1.
k. DN1 and ON2 receive PNT and go on hook
l. ON1 to DN1 call completes.
m. Place all instruments on hook.

2. Repeat test steps with the SUT as the DN.

Explicit Call Transfer (Unattended):

1. Place a PRIORITY call from ON1 to ON2.
   a. ON1 to ON2 call completes.
   b. ON1 transfers ON2 to ON1; don't answer.
   c. ON1 hangs up before DN1 answers; answer DN1.
   d. ON2 to DN1 call completes at PRIORITY.
   e. Place a ROUTINE call from ON1 to DN1.
   f. ON1 receives a standard busy tone.
   g. Place ON1 on hook.
   h. Place a PRIORITY call from ON1 to ON2.
   i. ON1 receives BPA or diverts appropriately.
   j. Place ON1 on hook.
   k. Place an IMMEDIATE call from ON1 to DN1.
   l. ON2 and DN1 receive PNT and go on hook.
   m. ON1 to DN1 call completes.
   n. Place all instruments on hook.
2. Repeat test steps with the SUT as the DN.

Data Required: Refer to Excel data collection form.

Test Procedure No: IO-2f
Requirement ID(s): SCM-000260, SCM-000270, SCM-000280, SCM-000290, SCM-000300, SCM-000310, SCM-000320, SCM-000330
Name: Three-Way Calling
Reference: UCR 2013 Sections: 2.2.6, 2.2.6.1
Applicability: SBC

Objective: SBCs must process Three-Way calls.

Test Setup:
1. All EIs used as conferee for this test procedure can have a dual appearance.
2. All EIs used as conferee should have a budget of at least 2.
3. Perform test procedures with the SUT as the ON and then repeat with the SUT as the DN.
4. TURN ON A PACKET CAPTURE PRIOR TO BEGINNING THE TEST PROCEDURE.

Test Procedures:

Inter-Environment:
Test Scenario for Station 1
1. Place a ROUTINE call from ON1 to DN1.
   ON1 to DN1 call completes.
   DN1 calls ON2 at PRIORITY, and then establishes a three–way call with ON1 and ON2.
2. Place a PRIORITY call from DN2 to ON1.
   ON1 receives PNT and goes on hook.
   DN1 and ON2 remain connected and both receive conference disconnect tone.
   DN2 to ON1 call completes.
3. Place all phones on hook.
4. Repeat test scenario incrementing precedence levels
   (i.e. R -> P, P -> I). Repeat test until second call is FLASH OVERRIDE.
5. Repeat test steps with the SUT as the DN.

Test Scenario for Station 2
1. Place a ROUTINE call from ON1 to DN1.
   ON1 to DN1 call completes.
2. DN1 calls ON2 at PRIORITY, and then establishes a three–way call with ON1 and ON2.
3. Place a PRIORITY call from DN2 to DN1.
   DN2 receives BPA or diverts appropriately.
4. Place DN2 on hook.
5. Place an IMMEDIATE call from DN2 to DN1.
   DN1 receives PNT and goes on hook.
   If DN1 is a proprietary EI (PEI), AND the three-way call bridge is NOT provided by the PEI, ON1 and ON2 remain connected and both receive conference disconnect tone.
   DN2 to DN1 call completes.
   If DN1 is a proprietary EI (PEI), AND the three-way call bridge IS provided by the PEI, ON1 and ON2 are disconnected.
   DN2 to DN1 call completes.
   If DN1 (the originator of the three-way call) is an AS-SIP EI (AEI), ON1 and ON2 are disconnected from the three-way call.
   DN2 to DN1 call completes.
6. Place all phones on hook.

7. Repeat test scenario incrementing precedence levels
   (i.e. R -> P, P -> I). Repeat test until second call is FLASH OVERRIDE.
8. Repeat test steps with the SUT as the DN.

Test Scenario for Station 3

1. Place a ROUTINE call from ON1 to DN1.
   ON1 to DN1 call completes.
2. DN1 calls ON2 at PRIORITY, and then establishes a three–way call with ON1 and ON2.
3. Place a PRIORITY call from DN2 to ON2.
   DN2 receives BPA or is diverted appropriately.
   Place DN2 on hook
5. Place an IMMEDIATE call from DN2 to ON2.
   ON2 receives PNT and goes on hook.
   DN1 and ON1 remain connected and both receive conference disconnect tone.
   DN2 to ON2 call completes.
6. Place all phones on hook
7. Repeat test scenario incrementing precedence levels
   (i.e. R -> P, P -> I). Repeat test until second call is FLASH OVERRIDE.
8. Repeat test steps with the SUT as the DN.

Data Required: Refer to Excel data collection form.

Test Procedure No: IO-3
Requirement: SCM-008680
Name: IEEE 802.1Q Support
Reference: UCR 2013 Section 2.17.7
Applicability: SBC

Objective: Determine if the SUT is capable of supporting the IEEE 802.1Q 2-byte TCI Field 12-bit Virtual Local Area Network Identification (VID)..

Test Setup:
1. Install a wire tap between the SUT and its Ethernet switch.
2. Connect a SIP capture tool to the wire tap.
3. Make sure the fronted SC and/or its end instruments are send packets tagged with a VLAN ID.
4. Perform test procedures with the SUT as the ON.

Test Procedures:
1. Start the AS-SIP signaling capture.
2. Make a call from ON1 on the LSC fronted by the SUT to DN1 off of another SC.
3. Verify bidirectional media flow.
4. Hang up all end instruments.
5. Stop the signaling capture.
6. Open an INVITE and expand the Ethernet Header.
7. Review the capture to ensure the following:
   a. The SUT received the VLAN ID from the LSC.
   b. The SUT forwarded the VLAN ID to the next SBC.

Data Required: Refer to Excel data collection form.

Test Procedure No: IO-4
Requirement: SCM-001770, SCM-001780, SCM-001790, SCM-001800, **SCM-001830,** SCM-001840, SCM-001850
Name: Network Interface (Management Functions)
Reference: UCR 2013 Section 2.7.1, 2.7.2, 2.7.4
Applicability: SBC

Objective: Determine if the SUT meets Ethernet interfaces Requirement.

Test Setup: NA

Test Procedures: Internal Interfaces
1. Verify with the vendor and review LOC to determine if the internal protocol used is proprietary or (IEEE) 802.3
2. Verify Ethernet interface is operational.
3. If the SUT uses 802.3, verify that they are capable of configuring the interface for auto-negotiation. This applies to all 10/100/1000BASE-T Ethernet standards
4. Access and log into the SBC Management via the Ethernet interface.
5. View the SBC configuration and status via the Ethernet interface.
6. Make changes to the SBC configuration via the Ethernet interface.
7. View the changes to the SBC configuration via the Ethernet interface.
8. Log off the SBC Management via the Ethernet interface.

Test Procedures: Interfaces to Switches and Routers
1. Verify with the vendor and review LOC to determine if the SUT support 10/100/1000BASE-T Ethernet physical interfaces to ASLAN switches and routers. 10GBASE-X is OPTIONAL.
2. If the SUT supports IEEE 802.3, verify it is capable of supporting auto-negotiation.

Test Procedures: Interfaces to VVoIP EMS
1. Verify with the vendor and review LOC to determine if the SUT supports 10/100BASE-X Ethernet physical interfaces to VVoIP EMS.
2. If the SUT must support either IEEE 802.3 auto-negotiation or IEEE Fast Ethernet 802.3u.

Test Procedures: Local Management Optional/Conditional requirements
1. **Optional:** The SUT has the option to use separate physical/redundant interfaces for Local Management and EMS Management.
2. If the SUT supports redundant interfaces, with separate bearer and signaling, verify that when the primary interface is broken, that signaling and bearer traffic failover to the secondary interface. This can be accomplished by disconnecting the primary interface.
3. **Conditional:** If the SUTs bearer traffic and signaling share a physical interface, verify that the bearer traffic and signaling use a separate VLAN.

Data Required: Refer to Excel data collection form.

Test Procedure No: IO-5
Requirement: SCM-008510, SCM-008520, SCM-008520.a, SCM-008520.b, SCM-008520.c, SCM-008530, SCM-008560, SCM-008570, SCM-008590, SCM-008690
Name: Media Anchoring
Reference: UCR 2013 Section 2.17.1
Applicability: SBC

Objective: Determine if the SUT meets back-to-back user agent and media anchoring requirement**.**

Test Setup:
1. Configure the SUT (SBC-2) as the SBC for the softswitch (SS-A). Refer to the test diagram provided in Figure 2.
2. Verify that LSC-A and LSC-B are both serviced SS-A.

Test Procedures:
1. Set up a signaling capture on SBC-2, or if necessary, have the vendor trace the call.
2. Place a call from ON1 to DN1.
3. Call completes. Verify the voice/video path is good in both directions.
4. Hang up all end instruments.
5. Stop the capture.
6. By processing the call between the fronted LSC and its associated SS, the SUT demonstrates that it supports B2BUA.
7. Review the captured call data.
   a. Verify that the “connection” (c=) line in the INVITE SDP received at SBC-2 from SBC-1 indicates the IP address of SBC-1.
   b. Verify that the “c=” line in the INVITE SDP leaving SBC-2 for SBC-3 has the same IP address as the SBC-1 WAN-side “c=” line.
   c. Compare the SUT’s incoming INVITE from SBC-1 to its outgoing INVITE to SBC-3. Ensure that the SUT decremented the “Max-Forward Header” count in the outgoing INVITE by 1.
   d. Compare the SUT’s incoming INVITE from SBC-1 to its outgoing INVITE to SBC
   e. Ensure that the SUT modified the CONTACT Header to reflect its IP address.
   f. Verify that the SUT preserved and passed the received Call Connection Agent Identifier (CCA-ID) in the CONTACT Header.
   g. Verify that the SUT maintained a continuous TLS session between SS-A and SS-B in both directions.
   h. Verify that the SUT processed packets within 2ms.

Repeat the procedure with DN1 calling ON1.
Repeat the procedure using all types of phones.

Data Required: Refer to Excel data collection form.

Test Procedure No: IO-6
Requirement: SCM-001170
Name: SC-Generated OPTIONS Failover/Failback (Alternative A) Scenario 1
Reference: UCR 2013 Errata 1, Section 2.6.1
Applicable UC Products: SBC

Objective: Verify that the SUT can support failover of an SC from the primary SS to a secondary SS using Alternative A: SC Generated Options Method

Test Setup:
1. Does the SUT support Alternative A? Y/N:
2. If yes, conduct both Alternative A and Alternative B test procedures. If No, go to Alternative B test procedures.
3. Configure the SUT to front an LSC that supports Alternative A (SC-Generated OPTIONS Method).

Note: This method is a function of the SC and includes OPTIONS pings from the SC with IP Destination Route headers beyond the SUT (i.e. the SS IP Header). Therefore, actual failover is not required to test this method.

Alternative A SC Generated Options Method Test Test Procedures:
1. Using a SIP capture tool at both the ingress and egress of the SUT, capture a successful OPTIONS ping from the fronted SC to the homed SS. Refer to Figure 5. for an example of an Alternative A OPTIONS ping.
2. Verify that the OPTIONS ping receives a response from the next AS-SIP appliance such as a “200 OK” or a “486-Too Many Hops”.

Data Required: Refer to Excel data collection form.

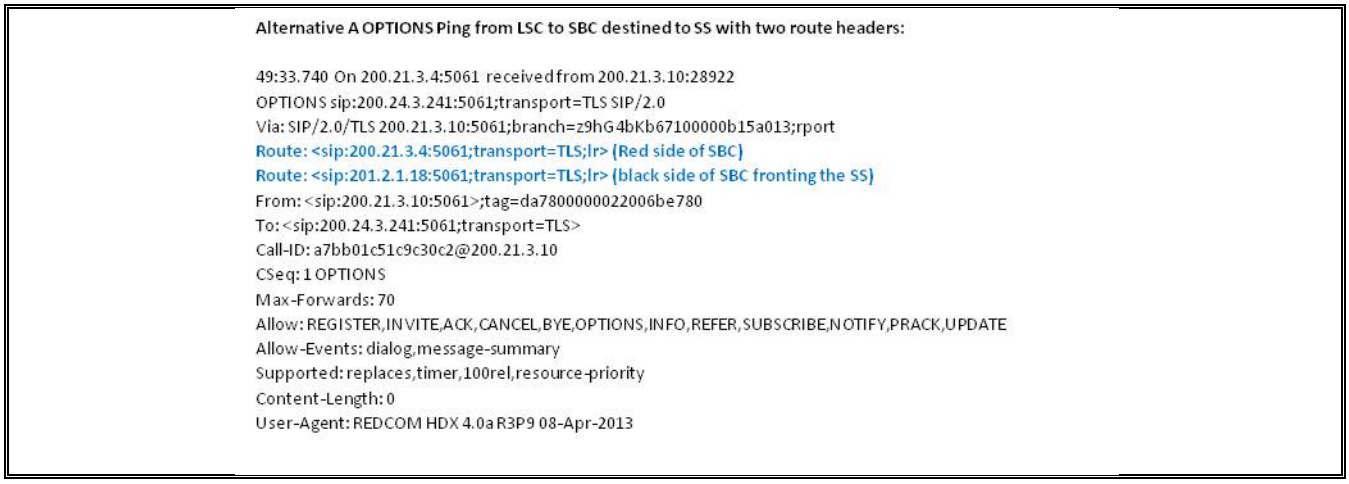


Figure 5. Alternative A OPTIONS Pings

Test Procedure No: IO-7
Requirement: SCM-001350, SCM-001360, SCM-001370, SCM-001380, SCM-001390, SCM-001400, SCM-001410, SCM-001420, SCM-001430, SCM-001440, SCM-001450, SCM-001460, SCM-001470, SCM=001480, SCM-001490, SCM-001500, SCM-001510, SCM-001520, SCM-001530, SCM-001540, SCM-001550, SCM-001560, SCM-001570, SCM-001580, SCM-001590, SCM-001600
Name: SBC-Generated OPTIONS Failover/Failback (Alternative B) Scenario 1, OPTIONS Pings Processed
Reference: UCR 2013 Errata 1, Section 2.6.2
Applicable UC Products: SBC

Objective: Verify that the SUT can support failover of an SC from the primary SS to a secondary SS using Alternative B: SBC Generated Options Method

Test Setup:
1. Does the SUT support Alternative B: Y/N
2. Configure the SUT to front an LSC that supports Alternative B (SC-Generated OPTIONS Method).

Note: This method is a function of the SC and includes OPTIONS pings between the SC and SBC and between SBCs.

Test Procedures:
1. Start the SIP capture tools
2. Review the capture for the following OPTIONs pings.
   a. Verify that the SUT received an OPTIONs ping from the fronted SC. Refer to Figure 6. for an example of an Alternative B OPTIONS ping**.**
   b. Verify that the OPTIONS ping received a response from the next AS-SIP appliance such as a “200 OK” or a “486-Too Many Hops”.
   c. Verify that the SUT sent a successful OPTIONS ping to the fronted SC. See Example below.
   d. Verify that the OPTIONS ping received a response from the next AS-SIP appliance such as a “200 OK” or a “486-Too Many Hops”.
   e. Verify that the SUT sent a successful OPTIONS ping to the SBC in front of the softswitch or distant SC. See Example below.
   f. Verify that the OPTIONS ping receives a response from the next AS-SIP appliance such as a “200 OK” or a “486-Too Many Hops”.

Alternative B OPTIONS Ping from SC to SUT:

39:36.636 On 200.30.3.4:5061 received from 200.30.3.10:1182
OPTIONS sip:NEC3C@dsn.mil:5061 SIP/2.0
Via: SIP/2.0/TLS 200.30.3.10:5061;branch=z9hG4bKf3ca84e0-88f5-41f1-864fc747d1ae6786
From: <sip:Sphericall@gntf.local>;tag=6dd7bb03-6027-4dff-ae104cc9bd4f40e7
To: "JITCEBC3" <sip:NEC3C@dsn.mil>
Contact: "ping" <sip:200.30.3.10;transport=tls>
Supported: presence,replaces,resource-priority
Route: <sip:200.30.3.4:5061;lr>
Route: <sip:201.2.1.4:5061;lr>
User-Agent: Sphericall/8.5.2 Build/430
Max-Forwards: 70
Call-ID: b9ccaf4c-d8ca-4203-886f006ec8bb1921@200.30.3.10
Content-Length: 0
CSeq: 33626 OPTIONS

Alternative B OPTIONS Ping from SUT to Fronted SC

23:31.174 On 200.20.3.4:19778 sent to 200.20.3.240:5061
OPTIONS sip:200.20.3.240:5061;transport=tls SIP/2.0
Via: SIP/2.0/TLS 200.20.3.4:5061;branch=z9hG4bKbo0tb4206g20unotr1i1
Call-ID: 098cee70028b71175b1a13a5a193f09a000mgh1@200.20.3.4
To: sip:ping@200.20.3.240
From: <sip:ping@200.20.3.4>;tag=a1625c09837a80cd7d3ba0f5314e8da3000mgh1
Max-Forwards: 0
CSeq: 2915 OPTIONS
Content-Length: 0

Alternative B OPTIONS Ping from SBC to SBC Fronting SS/SC

pd39:45.350 On 201.1.1.234:5061 received from 201.2.1.4:8208
OPTIONS sip:201.1.1.234:5061;transport=tls SIP/2.0
Via: SIP/2.0/TLS 201.2.1.4:5061;branch=z9hG4bKi0r22p100gm1slolg0k0
Call-ID: 003a060273997aaf91d7bed1da502c510000gl0@201.2.1.4
To: sip:ping@201.1.1.234
From: <sip:ping@201.2.1.4>;tag=a946885d1b2066b1e29445a75bc7c1880000gl0
Max-Forwards: 0
CSeq: 43 OPTIONS
Content-Length: 0

Figure 6. Alternative B OPTIONS Pings

Data Required: Refer to Excel data collection form.

Test Procedure No: IO-8
Requirement ID: SCM-008660, SCM-008670, SCM-001860, SCM-001870, SCM-001880, SCM-001890, SCM-001900
Name: Availability
Reference: UCR 2013, Errata 1 Section 2.8.2
Applicability: SBC

Objective: Session Border Controller must be able to meet the failover requirements as specified in the Unified Capabilities Requirements 2013 Errata 1 document. The subsystem(s) shall have no single point of failure that can cause an outage of more than 96 voice and/or video subscribers.

Test Procedures:
1. Review vendor Loc.
2. Inspect the SUT for anything that would cause a single point of failure for more than 96 voice and/or video subscribers.
3. Some examples of a single point of failure: lack of dual power supplies or any component /module that in the event of a catastrophic failure of the module/component would cause the SUT to become a single point of failure.

Data Required: Refer to Excel data collection form.

Test Procedure No: IO-9
Requirement ID: SCM-008660, SCM-008670, SCM-001860, SCM-001870, SCM-001880, SCM-001890, SCM-001900
Name: Product Quality Factors – Failover.
Reference: UCR 2013, Errata 1, Section 2.8.2
Applicability: SBC

Objective: SUT must be able to meet the failover requirements as specified in the UCR. The High Availability (HA) and Medium Availability (MA) Session Border Controller must be able to failover within 5 seconds or the result must be documented as a failure. The HA SBC must be able to also meet the *No Loss of Active Sessions* requirement. However, the MA SBC does not have to meet the "*No Loss of Active Sessions"* requirement part of this section.

Test Test Setup: NA

Test Procedures:
High Availability (HA) SBC Failover (Primary to Secondary Chassis Failover):
1. Ensure all configurations on the SBC(s) are saved before commencing the failover scenario (backed-up).
2. With the SUT connected to a SC, set up test measurement and diagnostic equipment (TMDE) such as a SAGE 960B (or equivalent test equipment) to an IP phone off of the SC and set the TMDE conduct a PVIT test. Place one other additional call.
3. Ensure that there is two-way audio and leave the phone calls up.
4. Run a 5-minute baseline PVIT test to ensure the test is running without any issues before performing the failover scenario. Record the results of the baseline into a folder for the SUT.
5. Fail the primary over to the secondary by disconnecting the power on the primary.
6. Record the results of the PVIT test and ensure the loss of audio is no longer than a total of 5 seconds.
7. Ensure all calls placed before the failover scenario is still up and did not disconnect. Check to ensure that two- way audio is present.
8. Ensure that additional calls can be placed 5 seconds after failover.
9. Record all results and place into a specially designated folder for the SUT.

Note: High Availability (HA) SBC: The system shall have an availability of 99.999 percent, including scheduled hardware and software maintenance (non-availability of no more than 5 minutes per year). The product shall meet the requirements specified in UCR 2013 and Product Quality Factors. The SUT must meet the *No Loss of Active Sessions* requirement (item i).

High Availability (HA) SBC Failback (Secondary to Primary Chassis Failback):
1. Ensure all configurations on the SBC(s) are saved before commencing the failback scenario (backed-up).
2. With the SUT connected to a SC, set up test measurement and diagnostic equipment (TMDE) such as a SAGE 960B (or equivalent test equipment) to an IP phone off the SC and set the TMDE conduct a PVIT test. Place one other additional call.
3. Ensure that there is two way audio and leave the phone calls up.
4. Run a 5-minute baseline PVIT test to ensure the test is running without any issues before performing the failback scenario. Record the results of the baseline into a folder for the SUT.
5. Fail the secondary over to the primary by disconnecting the power on the secondary.

6. Record the results of the PVIT test and ensure the loss of audio is no longer than 5 seconds.
7. Ensure all calls placed before the failover scenario are still up and did not disconnect. Check to ensure that two- way audio is present.
8. Ensure that additional calls can be placed 5 seconds after failback.
9. Record all results and place into a specially designated folder for the SUT.

Medium Availability (MA) SBC Failover (Primary to Secondary Chassis Failover) Dual Chassis Configuration:

1. Ensure all configurations on the SBC are saved before commencing the failover scenario (backed-up).
2. Place two phone calls up between SCs.
3. Ensure that there is two way audio and leave the phone calls up. The Medium Availability SBC does not have to maintain the "*no loss of active sessions"* requirement.
4. Fail the primary over to the secondary by disconnecting the power to the primary.
5. Calls are allowed to drop with a medium availability SBC.
6. Ensure that additional calls can be placed 5 seconds after failover.
7. Record all results and place into a specially designated folder for the SUT.

Note: Medium Availability (MA) SBC: Availability = 99.99 percent (52.5 min/year). The product does need to meet the requirements specified in Product Quality Factors with the following exception: The SUT does not have to meet the *No Loss of Active Sessions* requirement (item i). To meet medium availability SBC requirements the chassis must either have dual processors in a single chassis or have a single processor in a dual chassis configuration.

Test Procedures for a Medium Availability (MA) SBC Failback (Primary to Secondary Chassis Failover) Dual Chassis Configuration:

1. Ensure all configurations on the SBC are saved before commencing the failback scenario (backed-up).
2. Place two phone calls up between SCs.
3. Ensure that there is two way audio and leave the phone calls up. The Medium Availability SBC does not have to maintain the "*no loss of active sessions"* requirement.
4. Fail the secondary over to the primary by disconnecting the power to the secondary.
5. Calls are allowed to drop with a medium availability SBC.
6. Ensure that additional calls can be placed 5 seconds after failover.
7. Record all results and place into a specially designated folder for the SUT.

Data Required: Refer to Excel data collection form.

Test Procedure No: IO-10
Requirement ID: SCM-008660, SCM-008670, SCM-001860, SCM-001870, SCM-001880, SCM-001890, SCM-001900
Name: Product Quality Factors – Power Supply Failover.
Reference: UCR 2013, Errata 1, Sections: 2.8.2
Applicability: SBC

Objective: Session Border Controller must be able to meet the failover requirements as specified in the Unified Capabilities Requirements 2013 Errata 1 document. The High Availability (HA) and Medium Availability (MA) Session Border Controller must be able to failover within 5 seconds or the result must be documented as a failure. The HA SBC must be able to also meet the "*No Loss of Active Sessions"* requirement. However, the MA SBC does not have to meet the "*No Loss of Active Sessions"* requirement part of this section.

Test Setup:
Verify which of the following test cases applies to the SUT:

TEST CASE 1: Single Chassis Reliability: The SUT employs a single modular chassis to meet the reliability requirement. The SUT will have built-in back-up capability e.g., processors, power supplies, etc.).

TEST CASE 2: Duplicate System Reliability: The SUT employs a duplicate system to meet the requirement. The duplicate system may be in hot standby mode or active mode. The system, primary and secondary, must be sized to meet the engineered traffic load. The secondary system must be capable of taking over the functions of the primary system when the primary fails. High Availability SBCs will either come in a HA pair (dual chassis reliability) or be fully redundant in a single chassis configuration.

Note: Test Diagnostic Equipment must be able to perform the following test to measure failover: PVIT. A Packet Voice Interleave Test (PVIT) provides detailed diagnostic information about events that impact voice continuity to include the following: Voice frame losses, voice frame slips, voice clippings, and noise hits. Conducting a PVIT test will allow the tester to determine how long a loss of audio was during the failover scenario. The tester must ensure that the loss does not exceed 5 seconds.

Test Procedures for a High Availability (HA) SBC Power Supply Failover:
1. Ensure all configurations on the SBC(s) are saved before commencing the failover scenario (backed-up).
2. With the SUT connected to a SC, set up test measurement and diagnostic equipment (TMDE) such as a SAGE 960B (or equivalent test equipment) to an IP phone off the SC and set the TMDE conduct a PVIT test. Place one other additional call.
3. Ensure that there is two way audio and leave the phone calls up.
4. Run a 5-minute baseline PVIT test to ensure the test is running without any issues before performing the failover scenario. Record the results of the baseline into a folder for the SUT.
5. Check to see if the power supplies are hot swappable.
6. If the power supplies are hot swappable, then the tester will physically pull out the power supply. If the power supplies are not hot swappable, then the tester will pull the plug on only one of the power supplies.
7. A single power cord for multiple power supplies is a single point of failure and a TDR should be written.

8. Depending on whether the power supplies are hot swappable or not, either pull the primary power supply or pull the power cord on one power supply only.
9. Ensure that this does not cause the chassis to lose power.
10. Ensure all calls placed before the failover scenario is still up and did not disconnect.
11. Place the power supply back into the chassis or plug the power cable back in.
12. Ensure that placing the power supply back into the chassis or plugging the power cord back into the power supply does not cause a disruption in service.
13. Record all results and place into a specially designated folder for the SUT.

Test Procedures for a Medium Availability (MA) SBC Power Supply Failover:

1. Ensure all configurations on the SBC(s) are saved before commencing the failover scenario.
2. Place two calls up between the SCs.
3. Ensure that there is two way audio and leave the phone calls up.
4. Check to see if the power supplies are hot swappable.
5. If the power supplies are hot swappable, then the tester will physically pull out the power supply. If the power supplies are not hot swappable, then the tester will pull the plug on only one of the power supplies.
6. A single power cord for multiple power supplies is a single point of failure and a TDR should be written.
7. Depending on whether the power supplies are hot swappable or not, either pull the primary power supply or pull the power cord on one power supply only.
8. Ensure that this does not cause the chassis to lose power.
9. Ensure all calls placed before the failover scenario is still up and did not disconnect.
10. Place the power supply back into the chassis or plug the power cable back in.
11. Ensure that placing the power supply back into the chassis or plugging the power cord back into the power supply does not cause a disruption in service.
12. Record all results and place into a specially designated folder for the SUT.

Data Required: Refer to Excel data collection form.

Test Procedure No: IO-11
Requirement ID: SCM-008660, SCM-008670, SCM-001860, SCM-001870, SCM-001880, SCM-001890, SCM-001900
Name: SBC Link Failover
Reference: UCR 2013, Errata 1, Section 2.8.2
Applicability: SBC

Objective: Session Border Controllers must be able to meet the failover requirements as specified in the Unified Capabilities Requirements 2013 document. The High Availability (HA) and Medium Availability (MA) Session Border Controller must be able to failover within 5 seconds or the result must be documented as a failure. The HA SBC must be able to also meet the "*No Loss of Active Sessions"* requirement. However, the MA SBC does not have to meet the "*No Loss of Active Sessions"* requirement part of this section.

Test Setup:
Verify which of the following test cases applies to the SUT:

TEST CASE 1: Single Chassis Reliability: The SUT employs a single modular chassis to meet the reliability requirement. The SUT will have built-in back-up capability e.g., processors, power supplies, etc.).

TEST CASE 2: Duplicate System Reliability: The SUT employs a duplicate system to meet the requirement. The duplicate system may be in hot standby mode or active mode. The system, primary and secondary, must be sized to meet the engineered traffic load. The secondary system must be capable of taking over the functions of the primary system when the primary fails. High Availability SBCs will either come in a HA pair (dual chassis reliability) or be fully redundant in a single chassis configuration.

Notes:
1. Red Side: The side that faces the SC (LAN side).
   Black Side: The side that faces the CER (WAN side)

2. Test Diagnostic Equipment must be able to perform the following test to measure failover: PVIT. Note: A Packet Voice Interleave Test (PVIT) test provides detailed diagnostic information about events that impact voice continuity to include the following: Voice frame losses, voice frame slips, voice clippings, and noise hits. Conducting a PVIT test will allow the tester to determine how long a loss of audio was during the failover scenario. The tester must ensure that the loss does not exceed 5 seconds.

Test Procedures for a High Availability (HA) SBC Link Failover (Red Side) Single Chassis:
1. Ensure all configurations on the SBC(s) are saved before commencing the failover scenario With the SUT connected to a SC, set up test measurement and diagnostic equipment (TMDE) such as a SAGE 960B (or equivalent test equipment) to an IP phone off of the SC and set the TMDE conduct a PVIT test. Place one other additional call.
2. Ensure that there is two way audio and leave the phone calls up.
3. Run a 5-minute baseline PVIT test to ensure the test is running without any issues before performing the failover scenario. Record the results of the baseline into a folder for the SUT.
4. Unplug or disable the distant end red side connection of the SBC.
5. Measure the time it takes for the SBC to failover.

6. If the measured time is greater than 5 seconds, write a TDR.
7. Ensure all calls placed before the failover scenario is still up and did not disconnect.
8. Place new calls and ensure calls can be placed 5 seconds after failover.
9. Record all results and place into a specially designated folder for the SUT.
10. If there are two red side links, repeat steps 2-9.

Test Procedures for a High Availability (HA) SBC Link Failover (Black Side) Single Chassis:

1. Ensure all configurations on the SBC(s) are saved before commencing the failover scenario With the SUT connected to a SC, set up test measurement and diagnostic equipment (TMDE) such as a SAGE 960B (or equivalent test equipment) to an IP phone off the SC and set the TMDE conduct a PVIT test. Place one other additional call.
2. Ensure that there is two way audio and leave the phone calls up.
3. Run a 5-minute baseline PVIT test to ensure the test is running without any issues before performing the failover scenario. Record the results of the baseline into a folder for the SUT.
4. Measure the time it takes for the SBC to complete link failover.
5. If the measured time is greater than 5 seconds, write a TDR.
6. Ensure all calls placed before the failover scenario is still up and did not disconnect.
7. Place new calls and ensure calls can be placed 5 seconds after failover.
8. Record all results and place into a specially designated folder for the SUT.
9. If there are two black side links, repeat steps 2-9.

Test Procedures for a High Availability (HA) SBC Link Failover (Red Side) Dual Chassis (HA Pair):

1. Ensure all configurations on the SBC(s) are saved before commencing the failover scenario
2. With the SUT connected to a SC, set up test measurement and diagnostic equipment (TMDE) such as a SAGE 960B (or equivalent test equipment) to an IP phone off the SC and set the TMDE conduct a PVIT test. Place one other additional call.
3. Ensure that there is two way audio and leave the phone calls up.
4. Run a 5-minute baseline PVIT test to ensure the test is running without any issues before performing the failover scenario. Record the results of the baseline into a folder for the SUT.
5. Unplug or disable the distant end red side connection to SBC A (active SBC in the pair).
6. Measure the time it takes for the SBC to complete link failover.
7. If the measured time is greater than 5 seconds, write a TDR.
8. Ensure all calls placed before the failover scenarios are still up and did not disconnect.
9. Place new calls and ensure the calls can be placed 5 seconds after failover.
10. Record all results and place into the results folder for the SUT.
11. With the PVIT test running, reconnect the red side cable or enable the red side interface.
12. Measure the failback time for the link.
13. If the time it takes the link to failback is greater than 5 seconds, write a TDR.
14. Repeat the complete link failover scenario on SBC B (HA pair).
15. Place new calls and ensure calls can be placed 5 seconds after failover.
16. Record all results and place into a specially designated folder for the SUT.
17. If there are two red side links, repeat steps 2-16 (for second link).
18. Capture all results and place into the specially designated folder for the SUT.

Test Procedures for a High Availability (HA) SBC Link Failover (Black Side) Dual Chassis (HA pair):

1. Ensure all configurations on the SBC(s) are saved before commencing the failover scenario
2. With the SUT connected to a SC, set up test measurement and diagnostic equipment (TMDE) such as a SAGE 960B (or equivalent test equipment) to an IP phone off the SC and set the TMDE conduct a PVIT test. Place one other additional call.
3. Ensure that there is two way audio and leave the phone calls up.
4. Run a 5-minute baseline PVIT test to ensure the test is running without any issues before performing the failover scenario. Record the results of the baseline into a folder for the SUT.
5. Unplug or disable the distant end black side connection to SBC A (active SBC in the pair).
6. Measure the time it takes for the SBC to complete link failover.
7. If the measured time is greater than 5 seconds, write a TDR.
8. Ensure all calls placed before the failover scenario is still up and did not disconnect.
9. Place new calls and ensure the calls can be placed 5 seconds after failover.
10. Record all results and place into the results folder for the SUT.
11. With the PVIT test running, reconnect the black side cable or enable the black side interface.
12. Measure the failback time for the link.
13. If the time it takes the link to failback is greater than 5 seconds, write a TDR.
14. Repeat the complete link failover scenario on SBC B (HA pair).
15. Place new calls and ensure calls can be placed 5 seconds after failover.
16. Record all results and place into a specially designated folder for the SUT.
17. If there are two black side links, repeat steps 2-16 (for second link).
18. Capture all results and place into the specially designated folder for the SUT.

Test Procedures for a Medium Availability (MA) SBC Link Failover (Red Side) Single Chassis:

1. Ensure all configurations on the SBC(s) are saved before commencing the failover scenario
2. Place two calls from the SC.
3. Ensure that there is two way audio and leave the phone calls up.
4. Unplug or disable the distant end red side connection to the SBC.
5. Measure the time it takes for the SBC to complete link failover.
6. If the measured time is greater than 5 seconds, write a TDR.
7. Place new calls and ensure that the calls can be placed 5 seconds after failover.
8. Reconnect the red side cable or enable the red side interface.
9. Measure the failback time for the link.
10. If the time it takes the link to failback is greater than 5 seconds, write a TDR.
11. Record all results and place into a specially designated folder for the SUT.

Test Procedures for a Medium Availability (MA) SBC Link Failover (Black Side) Single Chassis:

1. Ensure all configurations on the SBC(s) are saved before commencing the failover scenario
2. Place two calls from the SC.
3. Ensure that there is two way audio and leave the phone calls up.
4. Unplug or disable the distant end black side connection to the SBC.
5. Measure the time it takes for the SBC to complete link failover.
6. If the measured time is greater than 5 seconds, write a TDR.
7. Place new calls and ensure that the calls can be placed 5 seconds after failover.
8. Reconnect the red side cable or enable the red side interface.

9. Measure the failback time for the link.
10. If the time it takes the link to failback is greater than 5 seconds, write a TDR.
11. Record all results and place into a specially designated folder for the SUT.

Test Procedures for a Medium Availability (MA) SBC Link Failover (Red Side) Dual Chassis:

1. Ensure all configurations on the SBC(s) are saved before commencing the failover scenario
2. Place two phone calls from a SC.
3. Ensure that there is two way audio and leave the phone calls up.
4. Unplug or disable the distant end red side connection to SBC A (active SBC in the pair).
5. Measure the time it takes for the SBC to complete link failover.
6. If the measured time is greater than 5 seconds, write a TDR.
7. Ensure all calls placed before the failover scenario is still up and did not disconnect.
8. Place new calls and ensure that the calls can be placed 5 seconds after failover.
9. Record all results and place into the results folder for the SUT.
10. Reconnect the red side cable or enable the red side interface.
11. Measure the failback time for the link.
12. If the time it takes the link to failback is greater than 5 seconds, write a TDR.
13. Repeat the complete link failover scenario on SBC B.
12. Reconnect the red side cable or enable the red side interface.
13. Measure the failback time for the link.
14. If the time it takes the link to failback is greater than 5 seconds, write a TDR.
15. Repeat failback scenario for SBC B.
16. If there are two red side links, repeat steps 2-15 (for second link).
17. Record all results and place into a specially designated folder for the SUT.
18. Capture all results and place into the specially designated folder for the SUT.

Test Procedures for a Medium Availability (MA) SBC Link Failover (Black Side) Dual Chassis

1. Ensure all configurations on the SBC(s) are saved before commencing the failover scenario
2. Place two phone calls from a SC.
3. Ensure that there is two way audio and leave the phone calls up.
4. Unplug or disable the distant end black side connection to SBC A (active SBC in the pair).
5. Measure the time it takes for the SBC to complete link failover.
6. If the measured time is greater than 5 seconds, write a TDR.
7. Ensure all calls placed before the failover scenario is still up and did not disconnect.
8. Place new calls and ensure that the calls can be placed 5 seconds after failover.
9. Record all results and place into the results folder for the SUT.
10. Reconnect the red side cable or enable the red side interface.
11. Measure the failback time for the link.
12. If the time it takes the link to failback is greater than 5 seconds, write a TDR.
13. Repeat the complete link failover scenario on SBC B.
14. Reconnect the red side cable or enable the red side interface.
15. Measure the failback time for the link.
16. If the time it takes the link to failback is greater than 5 seconds, write a TDR.
17. Repeat failback scenario for SBC B.
18. If there are two black side links, repeat steps 2-17 (for second link).

Data Required: Refer to Excel data collection form.

Test Procedure No: IO-12
Requirement: SCM-005660, SCM-005670, SCM-005690, SCM-005700, SCM-005710, SCM-005720, SCM-005730, SCM-005740,
Name: ESC
Reference: UCR 2013, Errata 1, Section 2.12.4.2.1, 2.12.4.2.2, 2.12.4.2.3
Applicable UC Products: SBC

Objective: Verify that the SUT meets all the UC requirements when fronting an ESC

Test Setup: NA

Data Required: Refer to Excel data collection form.

TEST WRAP UP

Get a copy of the configurations of all components of the SBC. Get the model number and revision level of all components. This information will be needed for the certification letter. Preserve a copy of your standard load and standard measurement configurations. These configurations will serve as a useful starting point for future tests of the SUT. Copy all test files to the file system used by your organization to create a common repository for test results. At JITC, this is the "T" drive. Tear down all cable runs used during the test to free up patch panel space and cables. If appropriate, start drafting the certification letter. If DISA adjudications have not been completed for outstanding test discrepancy reports (TDRs), draft the impacted sections of the certification letter in red font to make it easy to find once adjudication results arrive.